1/2009

Datenschutz Nachrichten

32. Jahrgang
ISSN 0137-7767
9,00 Euro

Datenschutz - quo vadis?

BDSG-Änderung ■ Kreditkartendaten im Christstollenpaket ■ Datenschutzskandale durch unzureichende Datenschutzgesetze ■ Informationen bei Datenschutzvorfällen ■ Neue Befugnisse des BKA ■ Datenschutznachrichten ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Der Redaktion der Zeitschrift IT-Grundschutz, SecuMedia Verlag, vielen Dank für die Einwilligung zum Abdruck des Beitrages von Karin Schuler (Seite 4). Auch der TITANIC-Redaktion vielen Dank, siehe Seite 44.

Hinweis an unsere LeserInnen:
Dieses Heft enthält das Register des Jahres 2008.
Bitte beachten Sie die Beilage des Haufe Verlages und des Datakontext-Verlages.

Termine

Sonntag, 19. April 2009
DVD-Vorstandssitzung in Frankfurt/M
(Interessierte DVD-Mitglieder möchten sich bitte bei der Geschäftsstelle melden)

Mittwoch, 22. April 2009
RFID - heimliche Kontrolle per Chip!
Kassel , Beratungsstelle für Technologiefolgen und Qualifizierung
weitere Informationen siehe unter www.btq-kassel.de

Dienstag - Donnerstag, 12. - 14. Mai 2009
Das novellierte Bundesdatenschutzgesetz
Tagung SoliSeminar in Düsseldorf
weitere Informationen unter www.soliseminar.de

Dienstag - Donnerstag, 12. - 14. Mai 2009
11. Deutscher IT-Sicherheitskongress – „Sichere Wege in der vernetzten Welt“ in Bonn-Bad Godesberg
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Nähere Informationen unter www.bsi.de (Rubrik Veranstaltungen)

Mittwoch, 3. Juni 2009
BTQ-Datenschutz-Fachtagung 2009
Arbeitnehmerdatenschutz - aktuell!
Hannover, weitere Informationen unter www.btq.de

Mittwoch, 15. Juli 2009
Nominierungsschluss für die BigBrotherAwards 2009
Nähere Informationen unter www.bigbrotherawards.de/nominate

Dienstag - Donnerstag, 15. - 17. September 2009
Gläserne Belegschaften
Tagung dtb-Kassel
weitere Informationen unter www.dtb-kassel.de

Freitag, 16. Oktober 2009
Verleihung der Big Brother Awards
Bielefeld, weitere Informationen unter www.bigbrotheraward.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
32. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Bonner Talweg 33-35, 53113 Bonn
Tel. 0228-222498
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Hajo Köppen
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Bonner Talweg 33-35, 53113 Bonn
dana@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Sascha Hammel,
35398 Gießen
Hammelwood@web.de

Druck
Wienands Printmedien GmbH
Linzer Str. 140, 53604 Bad Honnef
wienandsprintmedien@t-online.de
Tel. 02224 989878-0
Fax 02224 989878-8

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos.
Ältere Ausgaben der DANA können teilweise noch in der Geschäftsstelle der DVD bestellt werden.

Leserbriefe
Leserbriefe sind erwünscht, deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Titelbild: Frans Jozef Valenta
Rückseite: Titanic Magazin

Editorial

LIDL, Deutsche Bahn, Telekom, Airbus und diverse Callcenter; um nur die Spitze des Versagensberges zu nennen. Bei einem gravierenden Datenschutzverstoß erwischt treten die Unternehmenssprecher und manchmal die Chefs – auch wenn sie dann zurücktreten – vor die Mikrofone und versprechen, künftig das Datenschutzrecht 150%-tig einzuhalten. Kaum ist das Bußgeld für den letzten Verstoß bezahlt, greift irgendwo jemand in eine Mülltonne und fördert Vermerke mit Gesundheitsdaten von Beschäftigten zu Tage. Oops, LIDL did it again!

Die Datenschutzskandale der letzten Zeit schreien geradezu nach einer grundlegenden Erneuerung des Datenschutzrechts. Aber auch Politik und Gesetzgeber verhalten sich eher zwiespältig: Vor den Mikrofonen hui, in den Gesetzentwürfen eher pfui. Über einige diese „Huis“ und „Pfuis“ wird in dieser DANA berichtet und auch kontrovers diskutiert.

Hajo Köppen

Autorinnen und Autoren dieser Ausgabe:

Karin Schuler
Beraterin für Datenschutz und IT-Sicherheit
Stellv. Vorsitzende der Deutschen Vereinigung für Datenschutz
schuler@datenschutzverein.de

Klaus Jürgten Roth
roth.licht@web.de

Ingrid Pahlen-Brandt
Datenschutzbeauftragte der Freien Universität Berlin
pahlen@zedat.fu-berlin.de

Marit Hansen
Stellv. Landesbeauftragte für Datenschutz Schleswig-Holstein
marit.hansen@datenschutzzentrum.de

Werner Hülsmann
Dipl. Inform., selbständiger Datenschutzberater Konstanz, Vorstandsmitglied des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. sowie der Deutschen Vereinigung für Datenschutz (DVD) e. V.
huelsmann@datenschutzverein.de

Sönke Hilbrans
Rechtsanwalt, Berlin
Vorsitzender der Deutschen Vereinigung für Datenschutz
hilbrans@diefirma.de

Karin Schuler

Gut gemeint …
Kommentar zu den Änderungen des BDSG

Nach zahlreichen Datenschutzverletzungen bei großen deutschen Unternehmen im vergangenen Jahr, wurden die Stimmen nach gesetzlichen Konsequenzen immer lauter. Dezember 2008 wurde das Bundesdatenschutzgesetz novelliert – die Kritik daran reißt aber nicht ab.

IT-Fachleute, Revisoren und Wirtschaftsprüfer kennen den Vorgang: Jahrelang hat man auf Missstände hingewiesen und Verbesserungsvorschläge gemacht – ohne Erfolg. „Zu teuer, zu umständlich, nicht durchsetzbar" schallte es einem von den Verantwortlichen entgegen. Schließlich kommt es, wie es kommen musste: der Misstand produziert einen kleinen oder größeren Skandal und plötzlich wimmelt es nur so von Einsichtigen. Hektische Betriebsamkeit wird öffentlich zelebriert und weder Geld noch Aufwand werden gescheut, um den entstandenen Schaden so schnell wie möglich zu begrenzen und für die Zukunft Vergleichbares auszuschließen.

Auch Datenschützer haben seit langem mit diesem Muster zu kämpfen. Die heftigen Datenschutzskandale der letzten Zeit haben im Sommer 2008 sogar das Bundesministerium des Innern (BMI) zu öffentlich demonstrierter Betriebsamkeit gezwungen. Leider weiß man, dass hektische Betriebsamkeit nach Skandalen und großem öffentlichem Druck meist nicht zu den besten, effizientesten und angemessensten Maßnahmen führt. Auch das BMI bildet da keine Ausnahme, wie man den verschiedenen Stadien der Referentenentwürfe und den heißen Diskussionen entnehmen konnte. Selbst nach mehreren Kommentierungs- und Nachbesserungsrunden stellt der Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften vom 10.12.2008 ein wildes Flickwerk dar.

Fast kann man sich schon gar nicht mehr erinnern, dass es einst eine Initiative zur Modernisierung des Datenschutzrechts gab. Der heutige unzumutbare und für Normalbürger völlig unverständliche gesetzliche Flickenteppich sollte in ein modernes Datenschutzrecht aus einem Guss überführt werden. Der Gesetzgeber hat in mehr als einer Legislaturperiode Versprechungen zur Umsetzung gemacht. Geschehen ist bis heute jedoch nichts. Stattdessen werden nun am alten Flickwerk weitere Läppchen angenäht, um die immer größer werdenden dünnen Stellen und Löcher notdürftig zu stopfen.

Flickwerk BDSG

Immerhin sind diese Flicken an der richtigen Stelle angebracht, sie betreffen die am lautesten in der Öffentlichkeit beklagten Kritikpunkte. So wird endlich der Kündigungsschutz des betrieblichen Datenschutzbeauftragten (bDSB) verbessert, um diesen in seiner Weisungsfreiheit und fachlichen Unabhängigkeit zu stärken. Das ist durchaus zu begrüßen, auch wenn nach Meinung vieler Fachleute die jetzt vereinbarten Änderungen in der Stellung des bDSB bei weitem noch nicht ausreichen. Das bisher in den Bereichen Werbung, Adresshandel und Markt- und Meinungsforschung vorherrschende Widerspruchsprinzip (opt out: solange der Betroffene nicht widersprach, durften seine Daten genutzt werden), soll grundsätzlich dem Einwilligungsprinzip weichen (opt in: Daten des Betroffenen dürfen nur nach und mit seiner ausdrücklichen Einwilligung verwendet werden). Die Qualität der endgültigen Regelung wird nur dann akzeptabel sein, wenn der Gesetzgeber sich nicht wieder von den erbosten Adresshandels- und Werbeverbänden vielfältige Ausnahmen vom Grundprinzip abschwatzen lässt. Ein Novum im deutschen Datenschutzrecht stellt das Vorhaben einer Meldepflicht dar. Hierdurch wird bei Datenschutzverstößen die verantwortliche Stelle verpflichtet, Aufsichtsbehörde und Betroffene zu informieren. Diese Pflicht soll auch im Geltungsbereich des Telemedien- und des Telekommunikationsgesetzes Anwendung finden. Vorbilder für diese Regelung finden sich vor allem in US-amerikanischen Staaten. Es gibt allerdings unter Datenschützern einen Dissens darüber, wie wirksam diese Maßnahme die Folgen von Datenschutzverstößen mildern kann.

Die vorgesehene Erhöhung der Bußgelder geht einher mit einer Erweiterung des Bußgeldkatalogs, der nun beispielsweise auch die fehlende, unvollständige oder fehlerhafte Auftragserteilung bei Outsourcing (Auftrags-DV) mit Bußgeld belegt. Die vorgesehenen Bußgeldbeträge werden etwas erhöht – der eigentliche Qualitätsgewinn besteht allerdings in der vorgesehenen Option, diese Beträge weiter zu erhöhen, wenn nur so der durch den Verstoß erlangte Gewinn abgeschöpft werden kann.

Das ebenfalls in der Novellierung untergebrachte Datenschutzauditgesetz wird weniger in der Öffentlichkeit als in der Fachwelt diskutiert. Grundsätzlich ist zu begrüßen, dass das seit Jahren im § 9a des BDSG angelegte Gesetz nun doch endlich noch initiiert wurde. Analysiert man jedoch, was nach Jahren der Fachdiskussion und Erfahrungen mit privaten und öffentlichen Datenschutzaudits in diesen Entwurf eingeflossen ist, kann man nur ernüchtert sein. Der Text trägt mehr als deutlich die Handschrift eines Autors, der weder praktische Erfahrung mit Audits noch Kenntnis über die in den letz-

ten Jahren geführten Fachdiskussionen hat: vermutlich eine der typischen Auswirkungen des eingangs beschriebenen Schnellschusseffekts.

Ungeeigneter Gegenstand

Beispielhaft seien zwei wesentliche Kritikpunkte herausgegriffen: Gegenstand des Audits sollen sowohl Datenschutzkonzepte verant wortlicher Stellen als auch informationstechnische Einrichtungen von Anbietern sein. Damit ist der mögliche Gegenstand eines Audits jedoch inhaltlich nicht annähernd ausreichend definiert. Wegen der Einschränkung auf Datenschutzkonzept und informationstechnische Einrichtungen ließen sich weder Webportale noch Online- Shops auditieren – Anwendungen, deren Datenschutzstandard Verbraucher heutzutage ganz besonders interessiert. Auch mindert die Einschränkung auf das Audit des Datenschutzkonzepts – ohne eine zumindest stichprobenartige Überprüfung der Umsetzung – den Wert des erteilten Zertifikats immens: Papier ist geduldig und das wahre Datenschutzniveau zeigt sich in der betrieblichen Umsetzung.

Insbesondere ist fragwürdig, dass der vorliegende Entwurf im Ergebnis vorsieht, das freiwillige Zertifikat bereits für die eigentlich selbstverständliche, bloße Gesetzeseinhaltung zu erteilen. Dies transportiert nicht nur eine falsche Botschaft, sondern stellt auch keinen Wert für Verbraucher dar. Der Gesetzentwurf sieht vor, dass in einem bürokratisch aufwändigen, inhaltlich jedoch wirkungslosen Verfahren eine verantwortliche Stelle das Führen eines Auditsiegels anmelden kann. Eine Überprüfung durch die zuständige Kontrollstelle erfolgt erst nachträglich und richtet sich nicht zuletzt nach deren Arbeitsbelastung und der Einschätzung der Sensibilität der verwendeten Daten. Die Kontrollstelle soll dafür einerseits „angemessen" von der verantwortlichen Stelle bezahlt werden, hat aber andererseits die Verpflichtung, jede Stelle zu auditieren die dies wünscht. Gleichzeitig soll sie den Kunden, der sie für diese Leistung bezahlt hat, unabhängig und sachlich korrekt prüfen. Man darf sich fragen, ob es wohl häufig vorkommen wird, dass eine vom Kunden bezahlte Kontrollstelle im Falle unzureichenden Datenschutzniveaus ein Siegel versagt. Das gewählte einstufige Konstrukt, bei dem keine Trennung zwischen Sachverständigen und der auditierenden Stelle besteht, hat nicht zu Unrecht in Fachkreisen den Ruf eines leicht korrumpierbaren und daher letztlich wertlosen Modells.

Anforderungen

Besser wäre es, nach bewährtem Modell und an internationalen Zertifizierungsnormen ausgerichtet, in einem zweistufigen Verfahren eine unabhängige Zertifizierungsstelle auf der Grundlage eines Sachverständigengutachtens über die Zertifikatsvergabe entscheiden zu lassen. Wenn es nicht gelingt, mit einem Auditgesetz der Sache angemessene Rahmenbedingungen zu schaffen, so scheint die Gefahr groß, dass ein resultierendes Zertifikat in der Öffentlichkeit als nicht aussagekräftig wahrgenommen wird. Ein solches Gesetz sollte folgende Vorgaben umsetzen:

- Der Gegenstand des Audits, also das Prüfobjekt, sollte vorrangig die Datenschutzorganisation der datenverarbeitenden Stelle sein.
- Ein Zertifikat (als Bescheinigung eines erfolgreichen Audits) darf nur bei Erreichen eines hohen Datenschutzniveaus erteilt werden. Die alleinige Erfüllung der gesetzlichen Vorgaben ist nicht zertifizierungsfähig.
- Die Durchführung eines Datenschutzaudits ist für die datenverarbeitende Stelle freiwillig.
- Die Zertifizierung einzelner Organisationseinheiten oder Anwendungen der datenverarbeitenden Stelle ist nicht wünschenswert, weil die Aussagekraft sehr begrenzt ist und die Gefahr besteht, dass das Zertifikat für ein bestimmtes System missbräuchlich für die datenverarbeitende Stelle insgesamt genutzt wird.
- Erteilte Zertifikate müssen ein Mindestmaß an Vergleichbarkeit zulassen, da sie sonst für Verbraucher oder sonstige Interessenten nur von geringem Wert sind.
- Es sollte ein einziges, gleiches Zertifikat für alle Arten von datenverarbeitenden Stellen geben, das eine gute Datenschutzorganisation und ein hohes Datenschutzniveau bescheinigt. Eine Aufteilung von Zertifikaten nach Branchen, Größe der Stelle oder Art der Datenverarbeitung würde eine für den Verbraucher nicht überblickbare Zersplitterung zur Folge haben.
- Bei der Gestaltung eines Datenschutzaudits sollten bisherige systematische und strukturierende Arbeiten (z. B. Rossnagel, Rechtgutachten zum Datenschutzaudit 1999) berücksichtigt werden.
- Sowohl die Durchführung der Zertifizierung als auch die Akkreditierung der Gutachter sollte durch eine Stelle erfolgen, die Erfahrung in der internationalen Normierung von Zertifizierungsprozessen mitbringt, aber nicht selbst am Wettbewerb teilnimmt.
- Begutachtung und Zertifizierung sollen durch voneinander unabhängige Instanzen erfolgen (zweistufiges Modell). Da ein schludriges und unambitioniertes Gesetz die Idee eines Datenschutzaudits in der Öffentlichkeit dauerhaft diskreditieren wird, erscheint derzeit ein vorläufiger Verzicht auf ein Auditgesetz als die bessere Lösung.

Quelle: Nachdruck aus
IT-Grundschutz Informationsdienst
Nr. 2, Februar 2009, Seite 6 - 8,
ISSN 1862-4375

Klaus-Jürgen Roth

Die Kreditkartendaten im Christstollenpaket

Das Postpaket

Das Jahr 2008 war das Jahr der kleinen und der großen Datenlecks – von Callcenter über Kontodaten bis Telekom und T-Mobile. Überall suppten unbeabsichtigt oder bewusst unzulässig personenbezogene Daten heraus – aus CD-ROM, dem Internet oder über sonstige elektronische Datenträger. Kurz vor Weihnachten wurde uns dann von der Frankfurter Rundschau (FR) die ultimative analoge Jahresendgeschichte beschert. Sie berichtete, dass ihr am Tag zuvor in einem Postpaket Zehntausende von Kreditkartendaten auf Mikrofiches in einem Postpaket zugespielt worden seien. Auf den Fiches waren auch Geheimnummern enthalten sowie Namensangaben mit Kreditkartendaten (Adresse, Karten- und Kontonummer) und Kontobewegungen (Bezahlvorgänge, Rücküberweisungen, Abwicklungen zwischen Banken und Firmen). Die Daten, die LBB sprach schließlich von 130.000 betroffenen Kreditkartenbesitzenden, waren hochaktuell und stammten teilweise vom August 2008. Enthalten war im Paket auch eine Rechnung des Finanzdienstleisters Atos Worldline (AWL) an die Landesbank Berlin (LBB). Die Landesbank Berlin ist mit ca. 1,95 Mio. KundInnen der bundesweit größte Kreditkartenanbieter und wickelt für eine Vielzahl von anderen Banken und Finanzanbietern das Kreditkartengeschäft ab. Betroffen waren daher von dem Datenleck auch KundInnen vom ADAC über Amazon bis XBox von Microsoft. Die FR-Redaktion übergab das Paket der Polizei für weitere Ermittlungen.

Mikrofiches

In einem ersten Kommentar meinte der Berliner Datenschutzbeauftragte (BlnBDI) Alexander Dix, es sei „äußerst ungewöhnlich“, dass Mikrofiches durch die Gegend geschickt würden. Ein Sprecher des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) bekräftigte, dass es nicht den aktuellen Sicherheitsvorschriften entspreche, wenn die LBB solche Datenmengen auf Mikrofiches speichert.

Mikrofiches sind nicht gerade ein moderner, aber wohl ein nützlicher Datenträger. In den 30er Jahren des letzten Jahrhunderts wurde der Mikrofilm in der Schweiz erfunden, daraus wurden später die Mikrofiches. Dabei handelt es sich um Filmfolien im Karteikartenformat, auf denen sich große Datenmengen in Miniaturform speichern lassen. Sie sind geeignet, Texte oder Bilder fotografisch für die Nachwelt zu erhalten. Mit speziellen Lesegeräten können die verfilmten Schriftstücke auf einfache Weise vergrößert werden. In Deutschland liegen zahlreiche kulturgeschichtlichen Dokumente auf Mikrofiche im Barbarastollen im Schwarzwald. Durch die digitalen Speichermedien sind Mikrofiches immer mehr in Vergessenheit geraten, bis der aktuelle Kreditkartendaten-Skandal sie wieder ans Tageslicht beförderte. Die LBB und Atos nutzten offensichtlich dieses Medium, das in Sachen Haltbarkeit und Lesbarkeit (im Zweifel mit einer Lupe) digitalen Formaten überlegen ist. Nicht überlegen sind Mikrofiches in Sachen Sicherheit. Daher kündigte Atos zwei Tage nach Bekanntwerden des Datenlecks an, es werde künftig CompactDiscs (CD) mit verschlüsselten Daten nutzen. Mittelfristig plane das Unternehmen außerdem Veränderungen in seiner Fahrzeugflotte. Für Transporte heikler Daten sollten künftig „Sicherheitsfahrzeuge“ eingesetzt werden.

Kreditkartendaten

Tatsächlich sind diese Daten von höchster Sensibilität, wie der Stellvertreter des BlnBDI, Hanns-Wilhelm Heibey, bestätigte: „Damit könnte man im Internet überall alles kaufen, wofür nicht ausdrücklich die Prüfnummer auf der Rückseite der Kreditkarte angegeben werden muss.“ Trost versprach der Umstand, dass im konkreten Fall die Bank voll für die Verluste hätte haftbar gemacht werden können und die LBB ihre Einstandsbereitschaft auch signalisierte. Die beteiligten Firmen hatten sich zuvor gegenüber ihren KundInnen schon sensibilisiert gezeigt. Die LBB hatte sich am 26.09.2008 an Kundinnen gewandt, Atos am 04.12.2008, wonach es „zur Zeit“ und „vermehrt“ zu Kreditkartenmissbrauch im Internet gekommen sei. Ein Sprecher der LBB bestätigte, dass sich die Zahl der Missbrauchsfälle seit anderthalb Jahren weltweit und auch bei der LBB deutlich erhöht habe, insbesondere im letzten Quartal 2008. Bezüglich der per Kuriersendung verloren gegangenen Daten konnte aber kein Missbrauch festgestellt werden. Doch sollen sich Kreditkartenbesitzer an die FR gewandt und von illegalen Abbuchungen bis zu 5.000 Euro von ihren Konten berichtet haben; nachdem sie - wie dargestellt - von der LBB oder Atos über die Unregelmäßigkeiten informiert worden waren. Es war aber nicht nachzuweisen, dass die illegalen Abbuchungen etwas mit den außer Kontrolle geratenen Mikrofiches zu tun hatten.

Der LBB-Sprecher Marcus Recher bestätigte, dass PINs auf den verlorenen Mikrofiches gespeichert seien. Es handele sich aber um Nummern, die nie aktiviert wurden, da sie nicht hätten zugestellt werden können, z.B. weil die Empfänger unbekannt verzogen waren. Sie würden zur Vernichtung an die Bank zurückgeschickt: „Wir können absolut ausschließen, dass eine aktivierte PIN abhanden gekommen ist, die mit einem laufenden Konto verbunden ist.“ Schon am Wochenende hatten Tausende Kunden der Berliner Sparkasse, die auch LBB-Kreditkarten herausgibt, versucht, ihre Konten zu sperren und über Stunden so das Callcenter lahmgelegt .

Mutmaßungen

Über die Hintergründe des Vorgangs bestand zunächst völlige Unklarheit. Die Polizei in Frankfurt vermutete zunächst, dass das Paket verloren wurde. „Erste Ermittlungen haben ergeben, dass der Inhalt des Pakets vollständig ist, so dass nicht sicher ist, ob die Daten tatsächlich in die Hände unberechtigter Personen gelangt sind.“ Es liege keine Erpressung vor. Über die Motive könne nur spekuliert werden. In Berliner Polizeikreisen wurde die Vermutung geäußert, es handele sich um einen Trittbrettfahrer, da es bereits kurz zuvor ein Datenleck gegeben habe. Als möglich galt auch, dass ein Wichtigtuer sich in den Medien in Szene setzen sollte. Eine weitere Überlegung war, dass jemand auf ein gefährliches Leck beim Datentransfer hinweisen wollte.

Die Politik reagierte umgehend. So forderte der Vorsitzende des Bundestags-Innenausschusses Sebastian Edathy eine Pflicht, Kundendaten immer zu verschlüsseln und jeden Zugriff zu protokollieren. Die innenpolitische Sprecherin der Grünen, Silke Stokar, kritisierte die Banken, die ihren Kunden einen sorgsamen Umgang mit Geheimnummern abverlangten, „während sie selbst völlig ungesichert und unverschlüsselt Massen von Daten durch die Gegend schicken“. Bundesjustizministerin Brigitte Zypries (SPD) forderte eine „lückenlose“ Aufklärung. Der Vorfall zeige, „dass uns das Thema Datenschutz weiter intensiv beschäftigen wird“. Sie kritisierte die Kontrollen der Länder. Diese müssten ihre Datenschutzbehörden personell besser ausstatten, damit sie ihren Aufgaben gerecht werden könnten. Unionsfraktionsvize Wolfgang Bosbach plädierte für eine rasche Verabschiedung der geplanten Datenschutzreform, da damit bundesweit ein Datenschutzauditverfahren begründet werde. So könnten Firmen, die ihren Kunden besondere Sicherheit garantieren, eine Gütesiegel erhalten. Nicht ganz sachbezogen verlangte Petra Pau aus dem Vorstand der Linken „ein Moratorium für alle elektronischen Großprojekte, die den Datenschutz gefährden“. Die innenpolitische Sprecherin der FDP-Bundestagsfraktion, Gisela Piltz, forderte Firmen auf, offen zu legen, „wenn sie die Verarbeitung sensibler Daten auf andere, externe Unternehmen übertrügen“.

Der BfDI Peter Schaar warf der LBB vor, sie habe „offensichtlich kein effektives Schutzsystem“ bei der Verarbeitung der Daten gehabt. In einer eilig einberufenen Sitzung des Datenschutzausschusses des Berliner Abgeordnetenhauses kritisierte auch Daniel Holzapfel vom BlnBDI die LBB. Aus den von der LBB vorgelegten Verträgen lasse sich nicht erkennen, dass die Bank ihre Sorgfaltspflichten gewahrt habe. Ungewöhnlich sei, dass der Finanzdienstleister offensichtlich durch ein selbst gewähltes externes Unternehmen kontrolliert werde. Damit werde die LBB ihrer Verantwortung für den heiklen Umgang mit nahezu 2 Mio. Kreditkarten nicht gerecht. Ein LBB-Sprecher konterte, dass Atos „mehrfach zertifiziert“ sei und „hohe Standards“ unterhalte.

Die Regelungen zur Sicherheit bei Datentransporten sind nicht gerade die neuesten. Es gibt da lediglich den § 9 BDSG, der keine spezifischen Anforderungen enthält außer der, dass die Daten nicht von Unbefugten lesbar sein dürfen. Von Verschlüsselung ist darin keine Rede. Dass Daten nicht in gesicherten Behältern, sondern in Pappkartons durch die Gegend gefahren werden, ist zwar, so Heibey, üblich und zugleich zumindest befremdlich: „Man war bisher der Meinung, dass das ausreicht; diese Meinung hat sich geändert.“ Die LBB habe ihm versichert, „künftig bei allen Transporten Änderungen vorzunehmen“. Als Realitätsbeschreibung, nicht Prognose, stellte Rouven Schellenberg von der FR fest: „Die Unternehmen bauen ihre Geschäftsfelder meist wesentlich schneller aus als die Schutzwälle für die Daten ihrer Kunden. Wo Marketing, Vertrieb und Verkauf schon meist 2.0-Qualität erreicht haben, da wird der Datenschutz noch oft in 1.0-Manier organisiert.“

Der Verlust der Kreditkartendaten warf ein Licht auf die Verwaltung und Abrechnung mit diesen Karten: Mehr als JedeR vierte Deutsche hat eine Kreditkarte. Ausgebende Stellen sind nicht immer Banken, sondern z.B. der ADAC oder die Fluggesellschaft Air Berlin. Den wenigsten KundInnen ist bewusst, wieviele und welche Unternehmen im Hintergrund beteiligt sind. Eine zentrale Rolle spielt dabei die Firma Atos Wordline mit ihren zwei deutschen Niederlassungen, eine davon in Frankfurt-Niederrad. Atos ist Teil des französischen Konzerns Atos Origin. Dieser Konzern setzt mit seinen weltweit 50.000 Mitarbeitenden jährlich 5,8 Mrd. Euro um. Atos wickelt elektronische Vorgänge ab, SMS-Angebote, Krankenkartendatenverwaltungen oder eben die Zahlungsabwicklung mit Kreditkarten und verwaltet natürlich auch die verwendeten Daten. Banken und Sparkassen haben ihr Kreditkartengeschäft weitgehend ausgelagert. Sie bestimmen zwar die Konditionen und Zahlungsvorgänge. Die Durchführung erfolgt aber durch Firmen wie Atos oder dem US-amerikanischen Konzern First Data. Diese Spezialisten bündeln gewaltige Datenmengen, verfügen über die nötigen Technologien und Rechenzentren und können so die Leistungen billiger erbringen.

Die Frankfurter Polizei tappte bei der Fahndung nach den Verursachern zunächst im Dunkeln. Sie bestätigte, dass, entgegen früherer Angaben der LBB, auch PIN-Angaben im Fund enthalten waren. Die LBB bestätigte und erläuterte, dass es sich dabei um acht Umschläge von „Adressrückläufern“ handele. Die Polizei vernahm die beiden Kurierfahrer. Nach FR-Informationen handelte es sich um Angestellte der in Neuenstein ansässigen Firma General Logistics Systems (GLS), die von Atos beauftragt worden war, die Daten von Frankfurt nach Berlin zu transportieren.

Das kurz vor Heiligabend präsentierte Ermittlungsergebnis hörte sich dann doch sehr nach Weihnachtsgeschichte an: Die Frankfurter Staatsanwaltschaft gab bekannt, dass Atos den Kurierdienst damit beauftragt habe, sechs Pakete mit den Mikrofiches an die Landesbank zu schicken. Der Kurierdienst hatte ein Subunternehmen mit dem Transport unterbeauftragt. Die Unterkuriere sollten auch ein Paket eines Stuttgarter Elektronikunternehmens an den Chefredakteur der FR mit einem Christstollen transportieren. Beim

Sortieren sei den Kurieren das Paket mit dem Stollen in die Hände gefallen. Die Kollegen, 27 und 35 Jahre alt, öffneten es „und nahmen den Inhalt an sich". Um ihren Diebstahl zu vertuschen, klebten sie auf eines der sechs für die LBB bestimmten Pakete das Etikett des Christstollen-Päckchens, das dann die FR erreichte. Die anderen 5 Pakete kamen in Berlin an: Staatsanwaltschafts-Sprecherin Doris Möller-Scheu: „Der Fall konnte dank des engagierten und personalintensiven Einsatzes des zuständigen Fachkommissariats schnell geklärt werden, das noch nie mit so großem Personalaufwand den Diebstahl eines Weihnachtsstollens zu ermitteln hatte." Den Fahrern werde nun der „Diebstahl einer geringen Sache" und eventuell das „Unterdrücken einer Postsendung" zur Last gelegt. Von Beginn an hätten sich die Ermittler gewundert, dass der Stuttgarter Absender nicht zum brisanten Inhalt des Pakets passte. FR-Chefredakteur Uwe Vorkötter kommentierte: „Unter Genussaspekten wäre mir der Stollen lieber gewesen, unter journalistischen Aspekten waren es die Mikrofiches." Er warnte aber davor, den Fall nun ins Lächerliche zu ziehen. Er zeige, wie leicht sensible Daten an Unbefugte gelangen können.

Ingrid Pahlen-Brandt

Datenschutzskandale durch unzureichende Datenschutzgesetze

Datenschutz in Deutschland ist Not leidend. Die Skandale der jüngsten Vergangenheit offenbarten diesen Mangel des Schutzes personenbezogener Daten. Aktuell die Datenschutz-Affäre der Deutschen Bahn AG.

Vorwürfe trafen regelmäßig die Verantwortlichen in Firmen. Der Skandal um die Rasterfahndung bei der Deutschen Bahn gipfelte in der Rücktrittsforderung gegen ihren Chef, gegen Hartmut Mehdorn.[1]

Doch es sind nicht die verantwortlichen Personen allein, die gescholten werden sollten. Mit verantwortlich ist insbesondere der Gesetzgeber, der zu lange seinen Verpflichtungen nicht oder nur unzulänglich nachgekommen ist:

Die Versäumnisse des Gesetzgebers bezüglich wirksamer Datenschutzkontrolle – ihnen kommt die zentrale Rolle bei den Skandalen zu – sind bereits beschrieben[2], seine Versäumnisse beim Schutz von Verbrauchern und Arbeitnehmern sind in der Diskussion. Nicht hinreichend Beachtung geschenkt wird jedoch seinen Versäumnissen beim Erlass von Erlaubnisnormen. Fehler werden beispielhaft am Berliner Hochschulgesetz dargestellt.

Rechtliche Ausgangssituation in Berlin - Verfassung von Berlin

In Berlin genießt das informationelle Selbstbestimmungsrecht sogar Verfassungsrang. In Artikel 33 der Verfassung von Berlin (VvB) ist es als Grundrecht festgeschrieben. Personenbezogene Daten dürfen hiernach nur mit Erlaubnis verarbeitet werden; erlauben kann sie der Betroffene, aber auch der Gesetzgeber, sofern dies im überwiegenden Allgemeininteresses erforderlich ist. Erlaubnisse bilden so das Rückgrat des Datenschutzes: Die Forderungen nach sicherer Datenverarbeitung und Datenschutzkontrolle knüpfen lediglich an die jeweiligen Erlaubnisse an, denn nur bei sicherer Datenverarbeitung lässt sich die Einhaltung der Erlaubnisse gewährleisten. Auch die Kontrolle ist auf die Erlaubnisse als Vorgaben, deren Einhaltung zu kontrollieren ist, angewiesen.[3]

Berliner Hochschulgesetz

Scheinbar hat der Berliner Hochschulgesetzgeber seine Aufgabe zur

1 WELT Online vom 16. Januar 2009; Reuters vom 5. Februar 2009

2 Ingrid Pahlen-Brandt, Sind Datenschutzbeauftragte zahnlose Papiertiger? DuD 2007, 24ff.; Lehren aus der aktuellen Telekom-Affaire HU-Mitteilungen 201, S. 4f.

3 Die Gesamtheit der technischen, rechtlichen und organisatorischen Maßnahmen zur Gewährleistung nur erlaubter Verarbeitung von personenbezogenen Daten wird mit dem Begriff „Datenschutz" bezeichnet. Geschützt wird das Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Anknüpfungspunkt sind Daten, doch geschützt wird durch die Gewährleistung dieses Freiheitsrechts die demokratische Ordnung der Gesellschaft.

Regelung der Verarbeitung Personen bezogener Daten an Hochschulen wahrgenommen, denn er hat in § 6 Abs. 1 Satz 1 Berliner Hochschulgesetz (BerlHG) Zwecke[4] aufgezählt, zu denen ihre Erhebung, Speicherung und Nutzung durch die Hochschulen zulässig ist; § 6 Abs. 1 letzter Satz BerlHG verpflichtet die Hochschulen zur Datensparsamkeit.

Ermächtigung der Hochschulen

Die Hochschulen sollen die Verarbeitung personenbezogener Daten zu den in § 6 Abs. 1 Nr. 2 bis 8 BerlHG genannten Zwecken in Satzungen regeln, soweit sie zum Erlass von Satzungen befugt sind, im Übrigen durch Richtlinie (§ 6b Abs. 2 S. 1 und 2 BerlHG).[5] § 6 b Abs. 2 Satz 3 BerlHG bestimmt u.a. ausdrücklich, dass insbesondere die Art der zu verarbeitenden Daten zu regeln ist.

Der Verzicht des Gesetzgebers auf die Bestimmung der Art der zu verarbeitenden Daten für die jeweiligen Zwecke stellt ein gravierendes Versäumnis dar, denn die von ihm durch die Verfassung aufgetragene Entscheidung, ob eine Verarbeitung von Daten im überwiegenden Allgemeininteresse liegt, kann nur anhand konkreter Daten entschieden werden. Anhand der Erlaubnis zur Verarbeitung personenbezogener Daten in Benutzungsregelungen wird dies deutlich:

§ 6 Abs. 1 Abs. 1 S. 2 Nr. 6 BerlHG sieht die Verarbeitung personenbezogener Daten zur Benutzung von Einrichtungen der Hochschulen vor. Benutzungsregelungen können jedoch mit unterschiedlicher Intensität in das informationelle Selbstbestimmungsrecht der Benutzer eingreifen. Die Verarbeitung des Namens kann ausreichend sein, eventuell ergänzt um Geburtsdatum oder Matrikelnummer. Gedacht werden könnte aber auch an die Verarbeitung eines Fotos. Chipkarten, versehen mit RFID-Chip, könnten eingesetzt werden; gefordert werden könnten Fingerabdrücke oder sogar ein Irisscan.

In der Entscheidung über den Zweck einer Verarbeitung liegt – das ist hier gut zu sehen – nicht zugleich die wertende Entscheidung, dass das überwiegende Allgemeininteresse die Verarbeitung auch biometrischer Daten erlaube. Aber auch das Verbot der Verarbeitung biometrischer Daten zu diesem Zwecke ist mit der Entscheidung über den Zweck noch nicht getroffen. Die gebotene Entscheidung ist noch offen, wenn lediglich der Zweck bestimmt wird.

Auch durch die Verpflichtung zur Datensparsamkeit hat der Gesetzgeber nicht die von ihm geforderte wertende Entscheidung getroffen; Datensparsamkeit betrifft die Quantität der zu verarbeitenden Daten.

Der Staat erfüllt durch die Gesetzgebung seine Aufgabe, Hüter des Gemeinwohls gegenüber Gruppeninteressen zu sein.[6] Das Gesetzgebungsverfahren gewährleistet einen öffentlichen Willensbildungsprozess unter Abwägung der verschiedenen, häufig widerstreitenden Interessen. Dieses Verfahren ist in der Demokratie üblich für die Regelung von Fragen des Zusammenlebens, die in der Verfassung offen gelassenen sind. Bezogen auf das informationelle Selbstbestimmungsrecht hat die Verfassung offen gelassen, welche Verarbeitung welcher Daten zu welchen Zwecken im überwiegenden Allgemeininteresse liegt. Diese Entscheidung muss der Gesetzgeber treffen.

Durch sein gesetzgeberisches Versäumnis versagt er allen Mitgliedern der Hochschule den ihnen grundgesetzlich garantierten Schutz des informationellen Selbstbestimmungsrechts; Datenschutz bleibt ihnen versagt.

Richtlinie oder Satzung

§ 6 b Abs. 2 Satz 1 BerlHG stellt Satzungen und Richtlinien in folgender Formulierung nebeneinander:

„Die Hochschulen regeln die Verarbeitung personenbezogener Daten zu den in § 6 Abs. 1 Satz 1 Nr. 2 bis 8 genannten Zwecken in Satzungen, soweit sie zum Erlass von Satzungen befugt sind, im Übrigen durch Richtlinien. Sie regeln insbesondere die Art der zu verarbeitenden Daten….“

Diese Formulierung erweckt den Eindruck, dass die Art der Daten in zulässiger Weise sogar in Richtlinien bestimmt werden dürften. Das stünde jedoch im Widerspruch zu dem Charakter von Richtlinien mit lediglich interner Wirkung; als bloße Verwaltungsvorschriften können sie Eingriffe nicht wirksam erlauben.[7]

Hochschulautonomie - Wissenschaftsfreiheit

Auch der Hinweis auf die Hochschulautonomie kann den Berliner Gesetzgeber nicht entlasten. Zwar können sich grundsätzlich Erlaubnisse aus Satzungsregelungen ergeben, doch - neben der soeben dargestellten ausdrücklichen Forderung in der Verfassung von Berlin nach einer Entscheidung durch den Gesetzgeber selbst - sprechen hochschulrechtliche Besonderheiten gegen die Zulässigkeit von Einschränkungen des informationellen Selbstbestimmungsrechts durch Satzungen der Hochschulen.

Für das Bundesverfassungsgericht ist es für die Anerkennung von autonom gesetzten Regelungen mit

---

4 Folgende Zwecke sind hier erfasst:
- Nr. 1 zum Zugang, zur Durchführung des Studiums, zur Prüfung und zur Promotion,
- Nr. 2 Organisation von Forschung und Studium
- Nr. 3 Aufgaben nach dem Hochschulstatistikgesetz
- Nr. 4 Evaluation von Forschung und Studium
- Nr. 5 Feststellung der Eignung und Leistung von Mitgliedern der Hochschule durch Organe, Gremien oder Kommissionen der Hochschule
- Nr. 6 Benutzung von Einrichtungen der Hochschulen
- Nr. 7 Durchführung von Aufgaben der akademischen Selbstverwaltung
- Nr. 8 zum Einsatz von Steuerungsinstrumenten, in besonderen Zielvereinbarungen, Leistungsbewertungen, Mittelvergabesystemen
- Nr. 9 Evaluierung der Umsetzung des Gleichstellungsauftrages

5 Richtlinien können als Regelungen mit lediglich interner Wirkung Eingriffe nicht wirksam erlauben. Auf sie wird im Folgenden daher nicht eingegangen.

6 BVeErfGE 33, 125 (158)

7 Simitis u. a. BDSG 5. Auflage 2003, Simitis zu § 1 Rdnr. 98

Eingriffscharakter wichtig, dass sie das Ergebnis eines demokratischen Willensbildungsprozesses im Inneren der Organisation sind.[8] Diese demokratische Legitimation fehlt jedoch den Hochschulsatzungen aufgrund der gesetzlich geregelten Vorrangstellung der Hochschullehrer.

Das Berliner Hochschulgesetz gewährt den Professoren ein bestimmendes Übergewicht in den Akademischen Senaten, in Fachbereichs- und Institutsräten (vgl. § 60 BerlGH zu Akademischen Senaten, § 70 BerlHG zu Fachbereichsräten und § 75 BerlHG für die Institutsräte). In diesen Gremien haben sie stets eine Stimme mehr als die anderen in den Gremien vertretenen drei Statusgruppen[9] gemeinsam.

Demokratische Prinzipien werden so eingeschränkt und ein gerechter Interessenausgleich ist unter diesen Umständen nicht gewollt. Es besteht dadurch die Gefahr, dass aus Gründen der Praktikabilität Freiheitsrechte der übrigen Hochschulangehörigen eingeschränkt werden.

In der Facharztentscheidung[10] hat das Bundesverfassungsgericht eine solche Versuchung für Verwaltungen beschrieben. Es führt hier zur Ermächtigung zum Erlass von Verordnungen aus, dass dieser Versuchung der Verwaltung – in Verordnungen praktisch-effiziente Regelungen auf Kosten der Bürger zu treffen – Artikel 80 Abs. 1 Satz 2 GG dadurch Rechnung trägt, dass es die Bestimmung von Inhalt, Zweck und Ausmaß vom Gesetzgeber selbst fordert. Eine vergleichbare ausdrückliche Vorgabe zur Einschränkung der Satzungsautonomie enthält die Verfassung von Berlin – wie auch das Grundgesetz - nicht. Gleichwohl gilt die Wissenschaftsfreiheit, aus der die Bestimmungen zur Hochschulautonomie abgeleitet werden, nicht ohne Grenzen.

8 Beschluss der Ersten Senats vom 13. Juli 2004 – 1BvR 1298, 1299/94, 1332/95, 613/97 Notarkassen, BVerfGE 33, 125 – Facharztentscheidung

9 Neben den Hochschullehrern gibt es die Gruppen der wissenschaftlichen Mitarbeiter, der Studierenden und der sonstigen Mitarbeiter.

10 BVerGE 33, 125

Grenzen der Wissenschaftsfreiheit

Aus der Wissenschaftsfreiheit folgt die Pflicht des Staates, durch geeignete organisatorische Maßnahmen dafür zu sorgen, dass das Grundrecht der freien wissenschaftlichen Betätigung soweit unangetastet bleibt, wie das unter Berücksichtigung der anderen legitimen Aufgaben der Wissenschaftseinrichtungen und der Grundrechte der verschiedenen Beteiligten möglich ist; die einzelnen Träger des Grundrechts, also jedenfalls die Professoren, haben einen Anspruch auf organisatorische Maßnahmen zum Schutze des grundrechtlich gesicherten Freiheitsraumes.[11]

Die Wissenschaftsfreiheit gilt jedoch nicht ohne Grenzen, auch weist das Bundesverfassungsgericht bereits in seinem Hochschulurteil hin.[12] Die Verpflichtung des Staates, das irgend erreichbare Maß an Freiheit der wissenschaftlichen Tätigkeit zu verwirklichen, trifft auf die natürlichen Grenzen, die sich aus dem Zusammentreffen der Anliegen mehrerer Grundrechtsträger und aus Rücksicht auf andere wichtige Gemeinschaftsinteressen ergeben. Hierfür steht auch die Feststellung des Bundesverfassungsgerichts, „Wissenschaftsfreiheit ist kein Recht …, das eine … Verfügungsmacht über den Freiheitsstatus der übrigen Hochschulmitglieder gewährt".[13]

Hochschulrechtliche Besonderheiten erlauben es dem Gesetzgeber somit nicht, seine Befugnis zur Einschränkung des informationellen Selbstbestimmungsrechts den Hochschulen zu übertragen.

Gewinn für die Hochschulen

Zwar ist die Verpflichtung der Hochschulen rechtswidrig, doch dem Wortlaut des Gesetzes nach sind sie zum Erlass von Regelungen verpflichtet. Diese Pflicht besteht seit dem 6. Dezember 2004, das den Erlass dieser Regelungen bis zum 31. Dezember 2006 fordert. Gleichwohl fehlen diese notwendigen Regelungen in großem Umfang in Berlin. Angesichts der Tatsache, dass die Verarbeitung zu den in § 6 Abs. 1 Satz 1 Nr. 2 bis 8 BerlHG genannten Zwecken fortwährend geschieht, ist das Fehlen sehr erstaunlich, denn die Praxis der Verarbeitung von Personendaten wäre ja lediglich in eine Regelung zu gießen. [14]

Fehlendes Interesse der treibenden Kräfte an den Hochschulen an datenschutzgemäßen Zuständen ist sicher einer der Gründe dieses datenschutzrechtlichen Missstands. Hinzu kommt die inhaltliche Ferne dieser Regelung zur Wissenschaft. Die Bestimmung der Daten, deren Verarbeitung im überwiegenden Allgemeininteresse zu den in § 6 Abs. 1 Satz 1 BerlHG genannten Zwecken liegt, hat keinen unmittelbaren Bezug zu den Kernaufgaben der Hochschulen, dem Forschen und der Lehre. So bedeutete dies eine Entlastung der Hochschulen und somit einen Gewinn, wenn der Gesetzgeber seine Aufgabe endlich selbst wahrnähme.

11 VerfGE 35, 79,149 (Hochschulurteil)

12 BVerfGE 35,79, 147f.

13 BVerfGE 56,79, 163

Verordnungs-ermächtigung

§ 6 b Abs. 1 BerlHG ermächtigt die für Hochschulen zuständige Senatsverwaltung zur Regelung der Verarbeitung personenbezogener Daten durch eine Rechtsverordnung zu den in § 6 Abs. 1 Satz 1 Nr. 1[15] genannten Zwecken. Es handelt sich um den Zugang, die Durchführung des Studiums, um Prüfung und Promotion. § 6 b Abs. 1 Satz 2 BerlHG fordert auch hier, insbesondere die Art der zu verarbeitenden Daten und die Löschfristen zu regeln.

Wie bereits oben festgestellt, hat der Gesetzgeber selbst neben den Zwecken, zu denen personenbezogene Daten verarbeitet werden dürfen, auch die Art der für diese Zwecke zu verarbeiten-

14 Vgl. Wettern, M.; Lerherevulation an Hochschulen, DANA 1/2008, 18 ff. zum Regelungsdefizit in Niedersachsen

15 Die Senatsverwaltung wird zudem zum Erlass einer Verordnung ermächtigt bezüglich der Verarbeitung der Daten durch die Studierendenschaft. Bleibt hier außer Betracht.

den Daten selbst festzusetzen. Der Gesetzgeber hat für jedes Merkmal zu entscheiden, ob seine Verarbeitung für den beabsichtigten Zweck im überwiegenden Allgemeininteresse erforderlich ist. Der Verordnungsgeber ist nicht befugt, wirksame Erlaubnisse zu Eingriffen in das Grundrecht der informationellen Selbstbestimmung zu regeln.

Das Berliner Hochschulgesetz verstößt durch diese Verordnungsermächtigung zugleich gegen Artikel 64 Abs. 1 Satz 2 VvB, nach dem eine wirksame Ermächtigung die Regelung von Inhalt, Zweck und Ausmaß im ermächtigenden Gesetz selbst verlangt. Hieran mangelt es, wenn dem Verordnungsgeber lediglich Zwecke benannt werden und die Regelung der Art dem Verordnungsgeber übertragen wird.

Fazit

Schnell sollte der Gesetzgeber tätig werden, um den Mitgliedern der Hochschule Datenschutz zu gewähren. Hiermit wäre sowohl den Hochschulen – diesen durch die Entlastung von der Pflicht, wissenschaftsferne Regelungen zu erlassen – als auch dem Datenschutz gedient. Für die Hochschulgremien sind die zu treffenden Entscheidungen offensichtlich vollkommen unerheblich, andernfalls hätten Sie innerhalb der vergangenen vier Jahre ihre Regelungspflicht erfüllt[16]. Werden die Gremien zum Erlass von Regelungen verpflichtet, an denen sie offensichtlich nicht interessiert sind, so schwächt das den Datenschutz, der dann als störende Formalie wahrgenommen werden kann, der Regelungen fordert, die keinen interessieren. Geschwächt wird der Datenschutz gegenwärtig auch dadurch, dass das Fehlen von Erlaubnisregelungen ohne Folgen bleibt. Sein Ziel, die Gewährleistung der Rechte und Freiheiten der Einzelnen im Interesse der Aufrechterhaltung freiheitlicher und demokratischer Verhältnisse, würde nur allzu leicht vergessen werden. Oder ist dieser Fall vielleicht sogar bereits eingetreten?

Doch nicht nur für den Hochschulbereich ist der Gesetzgeber aufgerufen zu prüfen, ob er alles Notwendige geregelt hat. Versäumnisse der beschriebenen Art gilt es auch in anderen Bereichen zu finden und nicht nur in Berlin zu beheben.

16 Wäre die Übertragung der Satzungsbefugnis nicht bereits aus anderen Gründen rechtswidrig, könnte angesichts der langen Dauer der Untätigkeit an die Verwirkung des Rechts der Satzungsgebung zu denken sein. Am 2. Dezember 2004 beschloss der Gesetzgeber das Gebot, Regelungen bis zum 31. 12. 2006 zu treffen. Die Hochschulen hatten somit zwei Jahre hierfür Zeit. Bis heute sind bereits vier Jahre vergangen, ohne dass an den Berliner Hochschulen Regelungen in nennenswertem Umfang ergangen sind.

Meldepflicht bei Datenschutzpannen: Ja, bitte oder nein, danke?

Als im August 2008 Meldungen über den Diebstahl von 41 Millionen Kreditkarten-Nummern in den USA hierzulande durch die Presse gingen, forderte der Bundesdatenschutzbeauftragte Peter Schaar, US-Amerikanischem Beispiel folgend, die Einführung einer Meldepflicht für Unternehmen bei Datenmissbrauch. In den USA gibt es in 44 Bundesstaaten eine Meldepflicht für Unternehmen, denen Personendaten gestohlen wurden.

Macht eine solche Informationspflicht bei Datenschutzpannen auch im deutschen Datenschutzrecht Sinn oder trägt sie zur Verbesserung des Datenschutzes eher nichts bei? Mit dieser Fragestellung beschäftigen sich die beiden folgenden Beiträge von Marit Hansen und Karin Schuler, wobei die Autorinnen zu unterschiedlichen Antworten kommen.

Marit Hansen

Informationen bei Datenschutzvorfällen: Ja, bitte!

Nach den Datenschutzgesetzen sind Daten verarbeitende Stellen für die von ihnen verarbeiteten personenbezogenen Daten verantwortlich. Ziel der Datenschutzgesetzgebung in Deutschland ist die Gewährleistung des Rechts auf informationelle Selbstbestimmung für jeden Menschen: Jeder soll wissen können, wer was wann über ihn weiß (BVerfG 1983). Dies ist nur möglich, wenn die geforderte Transparenz nicht nur die planmäßige Datenverarbeitung betrifft, sondern auch im Fall von Sicherheitsvorfällen und Datenschutzpannen die Information darüber umfasst, welche der eigenen Daten in unberechtigte Hände gelangt sind.

So forderte im November 2008 die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, „alle verantwortlichen Stellen – grundsätzlich auch alle öffentlichen Stellen – gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen.“ (DSB-Konferenz 2008).

Dass eine solche Informationspflicht nicht unrealistisch ist, zeigen die Erfahrungen aus den USA, wo sog. „Security Breach Notification Laws“ in der Mehrheit der Staaten gelten, die die Unternehmen verpflichten, bei Datenschutzpannen die Betroffenen – oder falls dies nicht möglich ist, die Öffentlichkeit – zeitnah zu informieren. Dabei wirkt diese Verpflichtung nicht nur im nachgelagerten Bereich, sondern sie motiviert Unternehmen dazu, durch Datensparsamkeit sowie technische und organisatorische Maßnahmen Datenschutzpannen bereits im Vorfeld zu verhindern (Schneier 2009). Um im Fall einer Datenschutzpanne sowie der verpflichtenden Benachrichtigung den Vertrauensverlust bei den Kunden zu minimieren, werden in zahlreichen Unternehmen präventiv Notfallpläne erarbeitet. Statistiken aus den USA zeigen übrigens, dass mehr Kunden abwandern, wenn ein Datenskandal ungesteuert durch die Medien veröffentlicht wird (Hanloser 2009).

Auch für Deutschland, wo im Entwurf zur Novelle des Bundesdatenschutzgesetzes ebenso wie bei der Umsetzung der EU-Vorgabe im Medienrecht Informationspflichten bei Datenschutzpannen vorgesehen sind, wird eine solche bußgeldbewehrte Verpflichtung Wirkung in vermutlich zwei Richtungen entfalten: Erstens werden Unternehmen stärker versuchen, gar nicht erst Datenschutzpannen entstehen zu lassen – in vielen der jüngsten Datenskandale waren die Datensicherheitsmaßnahmen mangelhaft gewesen. Und zweitens wird weniger vertuscht werden, weil dies ein erhebliches Bußgeld nach sich ziehen kann – hier sind die Aufsichtsbehörden gefragt.

Die für Deutschland diskutierten Mitteilungs- und Benachrichtigungspflichten sollen zunächst auf besonders sensible Daten, z.B. im Bereich Medizin oder bei Bank- und Kreditkarteninformationen, beschränkt werden, da man bei einer Ausdehnung auf weniger sensible Fälle einen kontraproduktiven Abstumpfungseffekt bei den Betroffenen fürchtet. Wichtig ist bei dem Umfang der Benachrichtigung von Betroffenen, dass sie nach Möglichkeit abschätzen können sollen, von wem welche rechtswidrige Nutzung ihrer Daten droht und ob gegenwärtig eine konkrete Gefahr besteht (Hanloser 2009). Ebenso sollen den Betroffenen konkrete Handlungsempfehlungen zur Schadensminimierung gegeben werden.

Ähnliche Überlegungen stammen auch aus der Arbeit in den EU-Projekten „PRIME – Privacy and Identity Management for Europe“[1] (2004-2008) und PrimeLife[2] (2008-2011), in denen Konzepte und Prototypen für ein nutzergesteuertes Identitätsmanagement entwickelt wurden und werden:

Herzstück des PRIME-Identitätsmanagementsystems ist nutzerseitig der sogenannte „Data Track“, in dem mitgespeichert wird, welche Transaktionen der Nutzer abgewickelt hat, bei denen seine personenbezogenen Daten eine Rolle spielten. Der „Data Track“ gibt also Anhaltspunkte darüber, was der Transaktionspartner über einen weiß. Diese Grundfunktionalität wurde nicht nur um einen Abgleich mit den serverseitigen Datenschutz-Policies und erste Ansätze zur automatisierten Rechtewahrnehmung erweitert, sondern es wurde auch ein „Security Feed“ integriert, mit dem sich Sicherheitsvorfälle melden und an den Nutzer kommunizieren ließen (Nageler 2006, Hansen et al. 2007), siehe Abb. 1.

In der Praxis könnte es diverse Newsfeeds mit Informationen zu Datenschutzpannen und Sicherheitsrisiken geben, die in einem standardisierten Format Meldungen an diejenigen Nutzer weiterleiten würden, die den jeweiligen Newsfeed abonniert hätten. Verfasser dieser Meldungen könnten beispielsweise die verantwortlichen Daten verarbeitenden Stellen, Computer Emergency Response Teams, Online-Redaktionen oder beliebige Organisationen oder Einzelpersonen sein, die mit einer digitalen Signatur die Authentizität der Meldungen bestätigten würden. Das Identitätsmanagementsystem des

1 http://www.prime-project.eu/

2 http://www.primelife.eu/

Nutzers würde dann die abonnierten Newsfeeds auslesen und lokal aus den Meldungen diejenigen ausfiltern, die für den Nutzer bedeutsam sind, z.B. weil sie Transaktionspartner des Nutzers oder von ihm eingesetzte Technik beträfen. Bei dem im Projekt entwickelten XML-Format wurde u.a. berücksichtigt, zu welchem Zeitpunkt ein Vorfall bemerkt wurde und ab welchem früheren Zeitpunkt das Problem vermutlich schon Bestand hatte. Außerdem war ein Feld vorgesehen, um den Nutzer darüber zu informieren, welche Aktivitäten er entfalten könnte, um das Risiko für seinen Datenschutz zu minimieren: Im Kontodatenskandal 2008 hätte man z.B. auf die Möglichkeit des Wechsels der Kontonummer oder auf das regelmäßige Kontrollieren der Kontoauszüge hinweisen können; bei einem Datenleck, das pseudonyme Profile betrifft, wäre ein möglicher Ratschlag, nicht mehr das entsprechende Pseudonym zu verwenden.

Wichtig ist eine für den Betroffenen verständliche Art der Information. Identitätsmanagementsysteme können ihn bei der Interpretation der Benachrichtigungen ebenso unterstützen wie Datenschutzbehörden, Verbraucherschützer oder andere Organisationen seines Vertrauens.

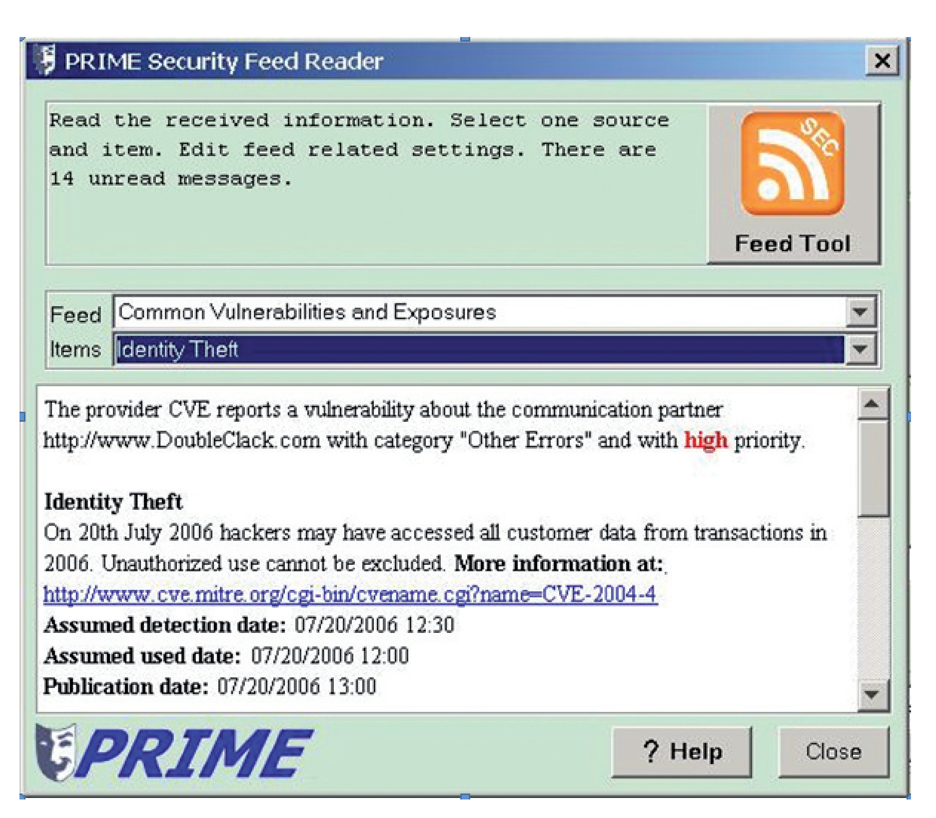


Abb. 1: Beispiel-Meldung im PRIME Security Feed

Fazit:

Eine Informationspflicht bei Datenschutzpannen ist notwendig, damit Bürgerinnen und Bürger ihr Recht auf informationelle Selbstbestimmung ausüben können. Voraussichtlich wird daneben der Grad der Datensicherheit in Unternehmen steigen. Insgesamt wird sich daraus eine Kultur für mehr Datenschutzbewusstsein und einen faireren Umgang mit Daten entwickeln.

Literatur

BVerfG 1983
Bundesverfassungsgericht: Urteil vom 15. Dezember 1983, BVerfGE 65, 1

DSB-Konferenz 2008
Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Mehr Transparenz durch Informationspflichten bei Datenschutzpannen; Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn (abrufbar beim Punkt „Entschließungen“ unter http://www.bfdi.bund.de/)

Hanloser 2009
Stefan Hanloser: Opt-out ist demnächst absolut out; InformationWeek, Ausgabe 1, 29. Januar 2009, S. 10-12

Hansen et al. 2007
Marit Hansen, Simone Fischer-Hübner, John Sören Pettersson, Mike Bergmann: Transparency Tools for User-controlled Identity Management; in: Paul Cunningham, Miriam Cunningham (Hrsg.): Expanding the Knowledge Economy: Issues, Applications, Case Studies; Proceedings of eChallenges 2007; IOS Press, Amsterdam 2007; S. 1360-1367

Nageler 2006
Antje Nageler: Integration von sicherheitsrelevanten Informationen in ein Identitätsmanagementsystem; Diplomarbeit am Institut für Informatik der Christian-Albrechts-Universität zu Kiel; Mai 2006

Schneier 2009
Bruce Schneier: Why security breach notification laws are a good thing, OUT-LAW News 17.02.2009; http://www.out-law.com/default.aspx?page=9800

Karin Schuler

Pseudo-Transparenz bei Datenschutzvorfällen: Nein, danke!

Auch wenn der vorliegende Text sich kritisch mit einer Meldepflicht für Datenschutzverstöße auseinandersetzt, soll keineswegs der falsche Eindruck entstehen, derartige Verstöße sollen bagatellisiert oder gar als nicht sanktionswürdig eingestuft werden. Das Gegenteil ist der Fall. Sanktionierung ist in weit höherem Maße erforderlich, als dies derzeit der Fall ist. Die Ursachen hierfür werden von Datenschützern seit langem öffentlich benannt und beklagt: Die abgrundtief schlechte Ausstattung der Aufsichtsbehörden und der für den öffentlichen Bereich zuständigen Beauftragten, die daher lächerlich lückenhaften Kontrollen, die halbherzige Absicherung betrieblicher Datenschutzbeauftragter und die putzigen, zu geringen Geldstrafen, die manches Unternehmen aus der Portokasse begleicht – wenn es denn überhaupt jemals auffällt.

Maßnahmen, die größere Gesetzestreue zum Schutz und Nutzen der Betroffenen erreichen, sind ohne Zweifel dringend erforderlich. Darunter fallen beispielsweise verbindliche Vorgaben für Schutz- und Schulungsmaßnahmen und die Stärkung des Datenschutzmanagements. Was ich allerdings für nicht wünschenswert hielte, wären Maßnahmen, die entweder diesen Zweck verfehlen, gar kontraproduktiv wirken oder beim Gesetzgeber Ressourcen binden, die für wichtigere gesetzgeberische Maßnahmen gebraucht würden. Inwieweit eine formalisierte Meldepflicht Unternehmen animiert, datenschutzgerechter zu agieren und dadurch die Betroffenenrechte stärkt, wird seit einiger Zeit diskutiert. Meine Bedenken gegen eine Meldepflicht resultieren im Wesentlichen aus der Befürchtung, ein inhaltlich richtiges Anliegen würde durch ein in der Praxis schwaches Instrument diskreditiert. Dies nicht zuletzt deshalb, weil von den wirklich dringenden Gestaltungserfordernissen im Datenschutz abgelenkt wird und, im Vergleich zu anderen, dringenderen Maßnahmen, nur ein schlechtes Kosten-Nutzen-Verhältnis erzielt würde.

Zu spät, zu teuer

Meldepflichten sind immer nachlaufende „Schadensbegrenzung“ und daher schlechter als jede vorbeugende Maßnahme. Mit begrenzten Ressourcen investiert man besser und effizienter in letzteres.

Datenschutz kämpft seit Jahrzehnten mit dem Mangel. Die Ausstattung betrieblicher Datenschützer und staatlicher Kontrollbehörden ist gleichermaßen schlecht. Für jede substantielle Verbesserung müssen Verteilungskämpfe um bessere personelle und finanzielle Ausstattung gefochten werden. Es wäre daher strategisch geschickt, mit den begrenzten Ressourcen (Zeit, Geld, Personal, Einfluss) vorrangig für Datenschutz-Maßnahmen zu streiten, die möglichst frühzeitig und effizient in betrieblichen und behördlichen Abläufen wirken, wie z. B. der vernünftigen Organisation des Kontrollwesens.

Zu theoretisch, zu kompliziert

Meldepflichten nutzen den Betroffenen nur, wenn diese mit der Meldung auch tatsächlich etwas anfangen können (ganz praktisch, nicht nur in der grauen Theorie). Dafür müssten sie die Meldung a) mitbekommen, b) verstehen, c) persönliche Konsequenzen abschätzen können und d) geeignete Maßnahmen ergreifen können. Wenig davon trifft für die Mehrzahl der Betroffenen zu. Verfügbare Schutzvorkehrungen im Internet (z. B. Mail-Verschlüsselung) sind bis heute ein Spielzeug für Spezialisten, was aus meiner Sicht beispielhaft den Kenntnisstand und das Bewusstsein der meisten Betroffenen widerspiegelt. Mit der Pseudo-Offenheit, mit der Datenschutzvorfälle bekannt gegeben würden, könnten ohne massive Sensibilisierungsbemühungen voraussichtlich nur wenige Betroffene etwas anfangen.

Zu nebulös, zu ungenau

Meldepflichten nutzen nur dann, wenn ihre Voraussetzungen eindeutig benennbar sind. So ist zum Beispiel ein meldepflichtiger Arbeitsunfall nachvollziehbar und eindeutig: Unfälle mit körperlichen Schäden während der Arbeitszeit lassen sich zweifelsfrei erkennen. Für Datenschutzvorfälle jedoch ergeben sich in der Praxis massive Abgrenzungsprobleme. Wie wird ein meldepflichtiger Vorfall definiert, wie also die Meldepflicht ausgelöst? Wer ist meldepflichtig (verantwortliche Stelle? Entdecker/Hacker? Aufsichtsbehörde?) und wie kann der meldepflichtigen Stelle nachgewiesen werden, dass sie Kenntnis hatte? Wie verhindert man, dass durch eine schlecht kontrollierte Meldepflicht letztlich die Vogel-Strauß-Politiker gewinnen (weil sie nicht öffentlich auffallen, weil sie keine aktive Fehlersuche betreiben) und sicherheitsbewusste Unternehmen durch aktives Sicherheitsmanagement evtl. Lecks entdecken, die ihnen dann öffentliche Aufmerksamkeit sichern?

Wenn sicherheits- und datenschutzbewusste Unternehmen jedoch die Dummen sind, wird ein Interesse ganz sicher weiter zunehmen: nämlich Vorfälle möglichst unter dem Deckel zu halten. Wie weit dieser Reflex schon heute verbreitet ist, lässt sich zum Beispiel daran ablesen, dass es keine seriösen, halbwegs repräsentativen Statistiken über Sicherheitsvorfälle gibt, die den Namen verdient hätten.

Die Meldung datenschutzrelevanter Vorfälle muss einen definierten, konkreten Nutzen für die Betroffenen haben, der über Schadenfreude, das Füllen von Zeitungsspalten, Datenschutzberichten

und Statistiken hinausgeht. Wie bereits dargestellt, ist ein wirklicher Nutzen für Betroffene fraglich. Die medialen Nebenwirkungen allerdings sind mit Sicherheit enorm und verstärken Vertuschungstendenzen.

Zu wirklichkeitsfern

Meldepflichten können nur dann wirken, wenn ein Verstoß dagegen ernsthaft strafbewehrt ist. Voraussetzung hierfür ist allerdings, dass Verstöße überhaupt bemerkt werden. Dies wiederum setzt in erster Linie ausreichende Ressourcen für die Überwachung/Aufsicht voraus. Wie soll die Einhaltung der Meldepflicht durch Aufsichtsbehörden kontrolliert werden, die heute noch nicht mal bemerken (wenn man von der Zahl von Unternehmen ohne Datenschutzbeauftragten ausgeht), wenn Unternehmen ihrer Meldepflicht gem. § 4 d BDSG nicht nachkommen? Und selbst wenn es gelänge, den jahrzehntelangen Kampf um mehr Ressourcen für die Aufsichtsbehörden positiv zu wenden, wären zuvörderst die bekannten und grundlegenden Missstände wirksam und flächendekkend zu kontrollieren: Missachtung der Pflichten zur Bestellung eines Datenschutzbeauftragten, zur Durchführung und Dokumentation innerbetrieblicher Vorabkontrollen, zur Erstellung eines Verfahrensverzeichnisses usw.

Kontraproduktiv

Sind Eindeutigkeit und Durchsetzbarkeit nicht gegeben, mutieren Meldepflichten zu einem Kampfinstrument im Wettbewerb. Das Ergebnis ist ein in höchstem Maße unfairer Zustand: Nicht diejenigen haben Vorteile, die die wenigsten Verstöße begehen bzw. erleiden, sondern diejenigen, die die besten Verschleierungstaktiken entwickeln. Und das erscheint aufgrund absolut mangelhafter Kontrollmöglichkeiten nicht schwer. Ein unerwünschtes Ergebnis könnte darin bestehen, dass Unternehmen zusätzlich in Verschleierungsmaßnahmen investieren und so die ohnehin schon schwierige Verfolgung von Verstößen zusätzlich erschweren.

Werner Hülsmann

EG-Richtlinie zur Vorratsdatenspeicherung ist auf eine geeignete Rechtsgrundlage gestützt

Am 10. Februar 2009 hat der Gerichtshof der Europäischen Gemeinschaften (EuGH) mit seinem Urteil die Nichtigkeitsklage Irlands und Sloweniens gegen die EG-Richtlinie zur Vorratsdatenspeicherung (Richtlinie 2006/24/EG) abgewiesen:
„Der Gerichtshof stellt zunächst klar, dass sich die von Irland erhobene Klage allein auf die Wahl der Rechtsgrundlage bezieht und nicht auf eine eventuelle Verletzung der Grundrechte als Folge von mit der Richtlinie verbundenen Eingriffen in das Recht auf Privatsphäre.
Der Gerichtshof stellt fest, dass die Richtlinie auf einer geeigneten Rechtsgrundlage erlassen worden ist.“[1]

Die Entscheidung betrifft – wie das Gericht selbst betont – nur die formale Frage der einschlägigen Rechtsgrundlage und hat die Verletzung der Grundrechte durch die anlasslose Erfassung des Telekommunikations- und Bewegungsverhaltens der gesamten Bevölkerung nicht zum Gegenstand.
Die mehr als 34.000 deutschen Beschwerdeführer/innen haben bereits beantragt, dass das Bundesverfassungsgericht den Europäischen Gerichtshof in einem zweiten Verfahren über die Vereinbarkeit der verdachtslosen Vorratsdatenspeicherung mit unseren Grundrechten entscheiden lässt. Daher ist das Urteil vom 10. Februar 2009 vermutlich nicht das letzte EUGH-Urteil in Sachen Vorratsdatenspeicherung.

1 Pressemitteilung des EuGH vom 10.02.2009 - http://curia.europa.eu/de/actu/communiques/cp09/aff/cp090011de.pdf

Werner Hülsmann:

Die neuen Befugnisse des Bundeskriminalamtes

Onlinedurchsuchung und Rasterfahndung durch das BKA – alles im Namen der Terrorbekämpfung

Nach kontroverser Diskussion im Bundestag, Bundesrat und in der Öffentlichkeit sind zum 01. Januar 2009 die neuen Befugnisse des Bundeskriminalamts (BKA) im BKA-Gesetz in Kraft getreten. Mit der im Dezember 2008 erfolgten Verabschiedung des „Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt“ im Bundestag und Bundesrat wurden dem BKA Polizeiaufgaben und damit u.a. die Befugnisse für Onlinedurchsuchungen und Rasterfahndungen übertragen.

Polizeiaufgaben und -befugnisse für das BKA

Bereits im Rahmen der ersten Stufe der Föderalismusreform aus dem Jahre 2006 wurde durch eine Grundgesetzänderung die Grundlage für die Erweiterung der Befugnisse des BKA gelegt. 1949 hatten die drei westlichen Besatzungsmächte auf Grund der Erfahrungen mit der Geheimen Staatspolizei (Gestapo) während der NS-Diktatur im sogenannten Polizeibrief[1] festgelegt, dass die Befugnisse einer Bundespolizei sich auf

„a) Überwachung des Personen- und Güterverkehrs bei der Überschreitung der Bundesgrenzen;

b) Sammlung und Verbreitung von polizeilichen Auskünften und Statistiken;

c) Koordinierung bei der Untersuchung von Verletzungen der Bundesgesetze und die Erfüllung internationaler Verpflichtungen hinsichtlich der Rauschgiftkontrolle, des internationalen Reiseverkehrs und von Staatsverträgen über Verbrechensverfolgung“[2] beschränken müssen. Die Trennung von Polizei und Verfassungsschutz wurde ebenfalls in diesem Polizeibrief niedergeschrieben:

„Der Bundesregierung wird es ebenfalls gestattet, eine Stelle zur Sammlung und Verbreitung von Auskünften über umstürzlerische, gegen die Bundesregierung gerichtete Tätigkeiten einzurichten. Diese Stelle soll keine Polizeibefugnis haben.“[3]

Allerdings haben die Regelungen des Polizeibriefs nach der Wiedererlangung der Staatssouveränität für den Gesetzgeber keine bindende Wirkung. Durch die neue Ziffer 9a im Artikel 73 Absatz 1 Grundgesetz (GG) erhielt der Bund die ausschließliche Gesetzgebung über „die Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalpolizeiamt in Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht“
(Art. 73 Abs. 1 Ziff 9a GG)

Vor der Einführung der neuen Ziffer 9a war das BKA in erster Linie zentrale Koordinierungsstelle des Bundes für polizeiliche Angelegenheiten. Das BKA wurde eingeschaltet, wenn mehrere Bundesländer befasst waren oder Straftaten bzw. Ermittlungen sich auf das Ausland bezogen. Daher hatte das BKA auch keine eigenen Eingriffsbefugnisse. Diese lagen alleine bei den Ländern und ihre Polizeibehörden. Ebenso war die Gefahrenabwehr alleinige Aufgabe der Länder. Hierfür haben die Strafverfolgungsbehörden der Länder die Befugnis, Verhöre, Durchsuchungen und Beschlagnahmen durchzuführen.

Durch das „Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt“ (BGBl. I S. 3083, 2008) wurde das BKA-Gesetz[4] erweitert und dem BKA nun Polizeiaufgaben und entsprechende Eingriffsbefugnisse gegeben.

Erweiterte Aufgabenstellung des BKA

Mit dem neuen „§ 4a Abwehr von Gefahren des internationalen Terrorismus“ im BKAG wurden die Aufgaben des BKA erweitert:

„Das Bundeskriminalamt kann die Aufgabe der Abwehr von Gefahren des internationalen Terrorismus in Fällen wahrnehmen, in denen

1. eine länderübergreifende Gefahr vorliegt,
2. die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist

oder

3. die oberste Landesbehörde um eine Übernahme ersucht.

Es kann in diesen Fällen auch Straftaten verhüten, die in § 129a Abs. 1 und 2 des Strafgesetzbuchs bezeichnet und dazu bestimmt sind, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale

1 Vgl.http://de.wikipedia.org/wiki/Polizeibrief

2 http://www.verfassungen.de/de/de49/grundgesetz-schreiben49-3.htm, 14.02.2009

3 http://www.verfassungen.de/de/de49/grundgesetz-schreiben49-3.htm, 14.02.2009

4 BKAG – online: http://www.gesetze-im-internet.de/bkag_1997/index.htm

Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können" (§ 4a, Abs. 1 BKAG).

Schon der zweite Satz zeigt deutlich, dass es um mehr geht, als nur um den internationalen Terrorismus. Vielmehr darf das BKA sich auch um terroristische Vereinigungen nach § 129a Strafgesetzbuch (StGB) kümmern. Die Ereignisse um den G8-Gipfel 2008 in Heiligendamm zeigen, dass die Bundesanwaltschaft in der Anwendung dieser Strafrechtsnorm nicht gerade zimperlich ist.

Die neuen Befugnisse des BKA

Neue Befugnisse erhielt das BKA durch Einfügung von 24 Paragraphen (§§ 20a – 20x BKAG). Die neuen Befugnisse, die bislang nur die Strafverfolgungsbehörden und Polizeibehörden der Länder hatten, sind insbesondere die Erlaubnis zur Erhebung persönlicher Daten sowie die Befragung, Vorladung und erkennungsdienstliche Behandlung von Personen (§§ 20b - 20f), die Befugnis zu Durchsuchungen von Sachen und Personen (§§ 20q, 20r), die Erlaubnis zur Erteilung von Platzverweisen (§ 20o), die Erlaubnis, Personen in Gewahrsam zu nehmen (§ 20p) und die Befugnis zur Sicherstellungen von Sachen (§ 20s).

Im Gegensatz zur polizeilichen Ermittlungsarbeit gilt bei Befragungen durch das BKA das Aussageverweigerungsrecht nur eingeschränkt. Wo nach Ansicht des BKA Gefahr für den Bestand des Staates oder Leib, Leben oder Freiheit einer Person besteht, müssen zukünftig Familienmitglieder gegeneinander, Rechtsanwälte gegen ihre Mandanten, Ärzte gegen ihre Patienten, Geistliche gegen ihre seelsorglich Bekannten aussagen.

Rasterfahndung

Auch das Mittel der Rasterfahndung wurde dem BKA an die Hand gegeben. So kann das BKA im Rahmen der erweiterten Aufgabenstellung auf richterlichen Beschluss eine Rasterfahndung durchführen und hierzu „von öffentlichen oder nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten von bestimmten Personengruppen aus Dateien zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen" (§ 20j, Abs. 1, 1. Halbsatz BKAG).

Onlinedurchsuchung – Onlineüberwachung

Mit der Neuregelung des BKA-Gesetzes hat das BKA die Befugnis erhalten, „verdeckte Eingriffe in informationstechnische Systeme" durchzuführen (vgl. § 20k BKAG). Hierdurch ist das BKA im Rahmen seiner Aufgaben nach § 4a BKAG befugt, mit technischen Mitteln (dem sogenannten „Bundestrojaner") in informationstechnische Systeme einzugreifen, um dort Daten zu erheben. Zu den informationstechnischen Systemen gehören dabei nicht nur PC, Laptop, Notebook und Netbook, sondern auch Mobiltelefone, Smartphones und PDA. Das Ausspionieren der Daten geschieht dabei nicht nur zu einem bestimmten Zeitpunkt, wie der Ausdruck Onlinedurchsuchung vermuten lässt, sondern kann über einen bestimmten Zeitraum erfolgen, so dass bereits bei dieser Regelung eher von einer Onlineüberwachung zu sprechen wäre. Im Gegensatz zu einer Hausdurchsuchung erfolgt die Onlinedurchsuchung heimlich. An das BKA übermittelt werden können dabei erstmal alle Dateien, auch solche, die offensichtlich als privat einzustufen sind und nichts mit dem Ermittlungsverfahren zu tun haben.

Hier ist – im Gegensatz zu anderen Befugnissen – der unbedingte Richtervorbehalt vorgesehen, d.h. eine ersatzweise Anordnung durch den BKA-Präsidenten oder bei Gefahr im Verzug ist nicht vorgesehen.

Überwachung der Telekommunikation

§ 20l des BKA-Gesetzes erlaubt es dem BKA im Rahmen des § 4a BKAG, die Telekommunikation Betroffener zu überwachen. Hierbei darf das BKA ebenfalls in informationstechnische Systeme eingreifen, z.B. PCs oder Mobiltelefone manipulieren, um die Telekommunikation direkt an der Quelle anzapfen zu können. So darf das BKA dann beispielsweise die Internettelefonate direkt auf dem PC des Betroffenen mitschneiden oder die verschlüsselt versendeten E-Mails auf dem Laptop des Überwachten im Klartext mitlesen. Derartige Maßnahmen sind von einem Richter anzuordnen, außer bei Gefahr im Verzug. Dann reicht für die ersten drei Tage die Anordnung durch den Präsidenten des BKA oder seines Vertreters.

Kritik am BKA-Gesetz

Ein wesentlicher Kritikpunkt an den neuen Befugnissen des BKA ist, dass der Kernbereich privater Lebensgestaltung, der nach der Verfassungsrechtsprechung unantastbar ist, durchlöchert wird. Insbesondere die Onlinedurchsuchung und -überwachung führen zur Verletzung dieses Kernbereichs. Die im BKA-Gesetz vorgesehene Regelung, dass die erhobenen Daten vom Datenschutzbeauftragten des BKA und zwei weiteren BKA-Beamten „auf kernbereichsrelevante Inhalte durchzusehen" sind, kann den Schutz des Kernbereichs privater Lebensgestaltung nicht sicher stellen.

Abgesehen von der Onlinedurchsuchung und -überwachung werden dem BKA-Präsidenten bzw. seinem Vertreter in vielen Bereichen Eilbefugnisse zugestanden, mit denen der Richtervorbehalt ausgehebelt werden kann. Auch dürfen Zweifel erlaubt sein, ob der Richtervorbehalt wirklich wirksam sein wird. Denn die Ablehnung eines derartigen Ersuchens ist detailliert zu begründen. Ob dies – selbst bei begründeten Zweifeln des Richters an der Zweckmäßigkeit, Verhältnismäßigkeit oder Angemessenheit – immer gelingt, ist mehr als fraglich.

Insbesondere die Regelungen

- § 20j Rasterfahndung
- § 20k Verdeckter Eingriff in informationstechnische Systeme
- § 20l Überwachung der Telekommunikation

stellen verfassungswidrige Eingriffe in das Fernmeldegeheimnis aus Art. 10 Grundgesetz (GG) sowie in das „Recht auf informationelle Selbstbestimmung" und das „Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" aus Art. 1 Abs. 1 GG in Verbindung mit Art. 2. Abs. 1 GG dar.

Die erste Verfassungsbeschwerde ist bereits am 27. Januar 2009 beim Bundesverfassungsgericht eingereicht worden[5]. Weitere Verfassungsbeschwerden wurden bereits angekündigt.

5 vgl. http://www.heise.de/tp/r4/artikel/29/29614/1.html, 14.02.2009 und http://www.bka-gesetz-stoppen.de, 14.02.2009

Sönke Hilbrans

Vor dem Ende einer kurzen Allianz?

Zum Beschluss des Verwaltungsgerichts Berlin zur Umsetzung der Vorratsdatenspeicherung vom 17.10.2008

Nicht erst seit einer Reihe von Datenschutzskandalen stehen InternetnutzerInnen, DatenschützerInnen und TelefonkundInnen der Telekommunikationsbranche nicht unbedingt freundlich gegenüber. Aber der Feind meines Feindes ist mein Freund, und so gab es Anlass für eine bemerkenswerte Allianz: Die Ablehnung der Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten. Nur wenige und kleine, meist idealistische Provider haben sich der juristischen Kampagne gegen die Vorratsdatenspeicherung angeschlossen, aber die lautstarke Kritik der Branchenverbände an den hohen Investitionskosten[1] wurden auch von der Seite der BürgerrechtlerInnen goutiert.

Vorratsdatenspeicherung vs. Berufsfreiheit

Das Verwaltungsgericht Berlin hat nun in einem viel beachteten Beschluss vom 17.10.2008[2] auf Antrag des deutschen Ablegers der British Telecom der Bundesnetzagentur untersagt, Zwangsmaßnahmen wegen der Nichterfüllung der mit dem für die Vorratsdatenspeicherung novellierten Telekommunikationsgesetz geschaffenen Vorratsdatenspeicherungspflicht zu ergreifen. Tragendes Argument des Gerichts ist insbesondere die Berufsfreiheit (Art. 12 Abs. 1 GG): Weil das geltende Telekommunikationsrecht (§ 110 Abs. 9 S. 2 TKG) eine Entschädigung für die Investitionen der Provider in Überwachungstechnologie nicht vorsieht, werden diese in ihrer Berufsausübung behindert. Dem klagenden Provider bleiben damit zunächst die aufzubringenden ca. 720.000,00 € Investitionskosten und 420.000,00 € jährliche Betriebskosten[3] für die Vorratsdatenspeicherung erspart. Es ist nicht der erste vorläufige Erfolg eines Providers gegen die Pflicht zur Umsetzung der Vorratsdatenspeicherung: Bei dem Bundesverfassungsgericht liegt bereits ein Vorlagebeschluss der gleichen Kammer des Verwaltungsgerichts Berlin vor, welcher ebenfalls die Verfassungswidrigkeit des Verzichts auf eine Entschädigungsregelung für Investitionskosten zum Gegenstand hat[4]. Mit der Telekommunikationsfreiheit der BürgerInnen hat das freilich nichts zu tun. Um Missverständnissen von vornherein zu begegnen, hat das Verwaltungsgericht

1 Nach heise online, Meldung vom 22.10.2008, 14:46 Uhr, taxiert Bitkom die notwendigen Investitionskosten der Telefonanbieter auf bis zu 75 Mil. € und schätzt der Branchenverband eco die notwendigen Investitionen der Internet-Wirtschaft in Hard- und Software sogar auf mind. 322 Mil. €.

2 Geschäftszeichen: VG 27 A 232.08; veröffentlicht u.a. in der kostenpflichtigen Datenbank www.juris.de

3 VG Berlin, B.v. 17.10.2008 - VG 27 A 232.08, Beschlussausfertigung S. 13 f.

4 Vorlagebeschluss v. 2.7.2008 – VG 27 A 3.07; Geschäftszeichen bei dem Bundesverfassungsgericht: 1 BvL 7/08; eine Entscheidung ist noch nicht bekannt geworden.

Berlin sogar ausdrücklich darauf hingewiesen, dass es weder die (von der Republik Irland vor dem Europäischen Gerichtshof angegriffene) Wirksamkeit der Vorratsdatenspeicherungsrichtlinie 2006/24/EG, noch die (vor dem Bundesverfassungsgericht mit zusätzlichen bürgerrechtichen Argumenten angegriffenen) Verfassungsgemäßheit der Umsetzung der Vorratsdatenspeicherung insbesondere in § 113a TKG thematisieren wollte.

Etappensieg für die Wirtschaft

Die politische Allianz von TK-Wirtschaft und NutzerInnen dürfte damit bröckeln: Viele Provider werden ihr Glück demnächst voraussichtlich auch lieber bei dem Verwaltungsgericht Berlin, denn in einer bürgerrechts- und datenschutzpolitischen Kampagne suchen. Dazu gibt die Entscheidung durchaus eine gute Basis her, auch für diejenigen, die nicht gleich eine dreiviertel Million bis zum Jahreswechsel hinblättern müssten, um der ungeliebten Pflicht nach der Vorratsdatenspeicherung nachzukommen. Freilich sind nicht alle Provider am Widerstand interessiert: Die Deutsche Telekom hat ihrerseits die immerhin 12 Millionen Euro teuren Investitionen in die Vorratsdatenspeicherung bereits weitestgehend getätigt[5]. Die Regierungskoalition hebt unterdessen zwar die Entschädigungstarife für die Mitwirkung an laufenden Überwachungsmaßnahmen an[6], was angesichts der überwältigenden Fallzahlen von TK-Überwachungsmaßnahmen und Standort-und Verbindungsdatenabfragen zusätzliche Millionen in die Kassen der Branche spülen dürfte[7], allerdings sind auch dabei keine Investitionsbeihilfen für die Telekommunikationsindustrie vorgesehen.

Bleibt die Entscheidung nur ein wirtschaftsliberales Manifest ohne Nährwert für die Auseinandersetzung um die Kernfrage, die bürgerrechtliche Erträglichkeit der Vorratsdatenspeicherung? Leider ist es so. Dabei liegt die Idee, dass den Netzbetreibern keine unprovozierten Opfergaben für staatliche Sicherheitsaufgaben abgenommen werden dürften, gar nicht so weit entfernt von dem auf den Grundrechten Datenschutz und Telekommunikationsfreiheit fußenden Argument, dass unbescholtene BürgerInnen auch keine Vorratshaltung ihrer Daten für zukünftige Sicherheitszwecke hinzunehmen hätten. Das Verwaltungsgericht Berlin hält sich nicht nur ausdrücklich aus dieser Debatte raus, es umgeht auch kunstvoll die augenfälligen Probleme, mit denen sich die Verfassungsbeschwerden gegen die Vorratsdatenspeicherung konfrontiert sehen. So kollidiere beispielsweise die Aussetzung der Umsetzungspflicht für British Telecom in Deutschland nicht mit der Vorratsdatenspeicherungspflicht nach der Richtlinie, denn die Bundesregierung könne durch eine Entschädigungsregelung ohne Weiteres Berufsfreiheit und Speicherungspflicht wieder in Einklang bringen. Das stimmt, aber der Flurschaden der Vorratsdatenspeicherung für die Bürgerrechte ist auch nicht in Geld zu entschädigen. Provider müsste man sein …

---

5 Heise online, Meldung vom 28.11.2008, 10:03 Uhr. Andere Unternehmen, welche vor allem ein Massenendkundengeschäft beschreiben, schätzen ihre Aussichten im einstweiligen Rechtsschutz offenbar skeptisch ein.

6 Gesetzentwurf: Bundtags-Drucksache 16/7103 v. 13.11.2007

7 Auch die neuen Tarife sollen nach dem Vorbringen der Bundesregierung gegenüber dem Verwaltungsgericht Berlin nicht kostendeckend ausfallen, mithin erst recht nicht die Investitionskosten decken, s. VG Berlin, B. v. 17.10.2008 – VG 27 A 232.08, Beschlussausfertigung S. 9. Von verurteilten Straftätern kann die Justiz die Entschädigungen mit den Verfahrenskosten zurückverlangen.

Datenschutznachrichten

Deutsche Datenschutznachrichten

Bund

Bahn spitzelte eigene Mitarbeiter aus

Im Kampf gegen Korruption hat die Deutsche Bahn von einer Detektei mehr als 173.000 ihrer insgesamt 240.000 Mitarbeiter ausforschen lassen. Zunächst wurde bekannt, dass ca. 1.000 Personen betroffen waren, vor allem Angehörige des oberen Managements und deren Ehepartner. Die Bahn hatte hierfür die Firma Network Deutschland GmbH eingeschaltet, d.h. dieselbe Detektei, die auch bei der Telekom für Spitzeldienste eingesetzt wurde. Die Konzernrevision der Bahn beauftragte Network zuletzt 2007. Es waren insgesamt 43 Operationen, mit denen Network für die Bahn in den vergangenen 10 Jahren im Namen der Korruptionsbekämpfung die eigenen MitarbeiterInnen ausgespäht haben soll, teils präventiv und ohne konkreten Anlass, mit Bezeichnungen v.a. aus Flora und Fauna: Uhu, Kabeljau, Thymian, Rosmarin, Basilikum oder Flieder.

Eine der verdeckten Aktionen bei dem Logistik-Riesen trug den Decknamen „Eichhörnchen“: Im Jahr 2003 erhielt die Firma Network den Auftrag, auszukundschaften, ob Top-Management oder Ehepartner außerhalb des Unternehmens wirtschaftlich engagiert sind. Es bestand kein konkreter Verdacht; die Ermittlungen waren pauschal angelegt. Die Revision der Bahn reichte zu diesem Zweck eine CD-ROM mit den persönlichen Daten von 774 Führungskräften an die Detektei weiter, darunter Personalnummern, Anschriften, Telefonnummern. Die Namen von 500 Ehepartnern beschaffte der Konzern ebenfalls und gab sie heraus. Im Personalregister der Bahn sind solche Angaben nicht zu finden; die internen Fahnder bezogen sie aus einer Kundendatei: Viele Führungskräfte hatten für ihre Partner verbilligte Fahrkarten bestellt und die Namen registrieren lassen. Network verglich die Personaldaten dann mit Angaben in öffentlichen Firmenregistern.

Kurz nach der Bekanntgabe der Bespitzelungsaktion wurde anlässlich eines Berichts vor dem Verkehrsausschuss des Deutschen Bundestags, dem der Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) Dix einen 7-seitigen Bericht vorlegte, bekannt, dass in den Jahren 2002 und 2003 die Bahn an Network Daten von 173.000 Beschäftigten weitergegeben hatte. Anhand von Adressdaten und Bankverbindungen sollte das Detektivbüro überprüfen, ob Mitarbeiter mit Scheinfirmen Geschäfte zu Lasten der Bahn abwickelten. Hierfür wurden die Daten mit denen von 80.000 Lieferanten abgeglichen. Gemäß bahninternen Unterlagen hat das Screening zwischen Lieferanten und Mitarbeitern unter dem Decknamen „Babylon“ ca. 300 Treffer gebracht. 125 davon gerieten unter verschärfte Beobachtung. In der Auftragsbeschreibung der Detektei heißt es dazu, dass nach dem Adressabgleich der Auftrag „dahingehend erweitert“ worden sei, „auch die Bank- und Telefonverbindungen in die Untersuchung einzubinden.“

Anlass für „Uhu“ war der Verdacht der üblen Nachrede gegen Konzernchef Hartmut Mehdorn. Ein DB-Mitarbeiter soll unter falschem Namen in einem Brief an Finanzbehörden Mehdorn eines Steuerdelikts bezichtigt haben. In dem Brief seien Informationen enthalten gewesen, zu denen etwa 40 Bahn-Beschäftigte Zugang gehabt hätten, heißt es in dem Dix-Bericht. Network habe ein „Schriftstilgutachten“ anfertigen lassen, das zu einem DB-Mitarbeiter geführt habe, der gekündigt worden sei. Die Arbeitsgerichte hätten das Gutachten aber nicht anerkannt und die Kündigung aufgehoben. Gemäß dem Dix-Bericht wurden in diesem Fall „wahllos E-Mails der Betroffenen an Network übermittelt“, darunter Schreiben an den Betriebsrat und Informationen über Besprechungen beim Betriebsrat.

Gemäß dem Bericht des BlnBDI wurde der Betriebsrat „in keinem der Fälle“ über die Zusammenarbeit mit Network informiert. Die Bahn hatte vorgetragen, „man habe Zweifel an der Zuverlässigkeit bzw. Diskretion des (zu geschwätzigen) Betriebsrats“. Außerdem haben weder Network noch die Bahn nach Abschluss der internen Ermittlungen die betroffenen Mitarbeiter informiert. Die Bahn habe das „nicht für erforderlich gehalten, da die zu Unrecht Verdächtigen anschließend nicht benachteiligt worden seien“.

Dadurch, dass mit Network unter der Führung von Ralph Kühn ein Unternehmen beauftragt wurde, das auch für andere Großunternehmen spitzelte, wie z.B. für die Telekom, ist nicht ausgeschlossen, dass über die jeweiligen Konzerngrenzen hinaus ermittelt worden ist. Von 1998 bis 2007 kassierte Network allein von der Bahn für die Abarbeitung der 43 Aufträge 807.280 Euro.

Der für die Aufsicht des Konzerns zuständige Datenschutzbeauftragte Dix hält solche Späh-Aktionen für nicht rechtens: „Wir haben bei der Bahn erhebliche Verstöße gegen das Bundesdatenschutzgesetz festgestellt.“ Seine Behörde prüfe, ob das Unternehmen ein Bußgeld zahlen müsse. In einigen Fällen seien strafrechtliche Delikte nicht auszuschließen: „Wir prüfen, ob wir die Staatsanwaltschaft einschalten.“ In dem Bericht des BlnBDI werden neben den pauschalen Fahndungsaktionen zudem hausinterne Ermittlungen in Verdachtsfällen beschrieben. In einem Fall seien, so der Bericht, „wahllos E-Mails der Betroffenen an die Network Deutschland GmbH übermittelt worden“. Ein anderes Mal seien „private Geld- und Kontobewegungen sowie Reisetätigkeiten und Familienverhältnisse“ ermittelt worden.

Die Bahn räumte ein, dass es entsprechende Ermittlungsaktionen gab. Auch mögliche Probleme beim Datenschutz gibt der Konzern zu: „Seitens des Berliner Datenschutzbeauftragten wurde auf

mögliche formale Verstöße durch die Bahn hingewiesen, wie die fehlende Unterrichtung der Mitarbeiter nach durchgeführten Untersuchungen.“ Ein Vergleich mit Datenschutzskandalen - wie bei der Telekom - sei jedoch „völlig falsch und abwegig“, stellte die Bahn fest. Im Fall der überprüften Kontobewegungen gibt das Unternehmen an, die „privaten Kontoumsätze“ in einer Excel-Tabelle auf einem „Dienstrechner als Zufallsfund“ entdeckt zu haben. Die Berliner Datenschützer monierten, die Aufträge an Network seien nur mündlich übermittelt worden. Dies wird von der Bahn mit „der zeitlichen Dringlichkeit und der Sensibilität der Fälle“ erklärt. Die Revision der Bahn räumte außerdem ein: „Es trifft zu, dass der Betriebsrat aus Gründen der Vertraulichkeit nicht über die fallweise Zusammenarbeit mit Network informiert war.“

Um der Presseveröffentlichung am 21.01.2009 zuvor zu kommen, hatte die Bahn am Nachmittag vorher eine Pressemitteilung veröffentlicht: „DB und Berliner Datenschutzbeauftragter analysieren Arbeit der Network GmbH“. Darin behauptete die Bahn, dass die zuständige Aufsicht keine „grundsätzlichen Bedenken“ geäußert hätte, was vom stellvertretenden Berliner Datenschutzbeauftragten Thomas Petri dementiert wurde: „Die Darstellung der Deutschen Bahn trifft so nicht zu. Wir haben erhebliche Zweifel an der Rechtmäßigkeit der Datenverarbeitung bei der Bahn.“ Die DB konterte Medienberichte; ein Vergleich mit Lidl und Telekom sei „blühender Unsinn“, so Konzernsprecher Oliver Schumacher: „Die Deutsche Bahn war in den vergangenen zehn Jahren wiederholt Opfer schwerster Fälle von Wirtschaftskriminalität und Korruption. Ihr Kampf gegen diese Übel ist immer wieder als beispielhaft bewertet worden. Im Interesse aller ehrlichen Kunden, Steuerzahler und Mitarbeiter wird die DB AG im Rahmen der gesetzlichen Vorschriften weiterhin mit aller Härte gegen solche Auswüchse vorgehen, die das Gemeinwohl massiv schädigen.“ Wolfgang Schaupensteiner, Chief Compliance Officer der DB AG seit Juli 2007 und zuvor Oberstaatsanwalt und damit staatlicher Korruptionsbekämpfer in Hessen von 1987 an, ergänzte: „Der Hinweis auf mögliche Verstöße wird von uns ernst genommen. Es bestehen aber keine Anhaltspunkte für die Beteiligung von DB-Mitarbeitern an Straftaten“. Ziele der Beauftragung wären z.B. die Aufdeckung von Scheinfirmen und Kartellsachverhalten oder auch die Klärung des Verbleibs „mobiler Vermögensgegenstände“, z.B. Lokomotiven, gewesen. „Es wurden keine Telefone abgehört, keine Konten eingesehen, keine Journalisten abgehört“. Vielmehr seien nur die Daten, z.B. Adressen, Telefonnummern und Kontonummern, mit denen von Auftragnehmern „abgeglichen“ worden. Es habe „umfängliche Recherchen“ gegeben, was als „Monitoring“ auch sinnvoll sein. In den Fällen, in denen sich Interessenkonflikte ergeben hätten, seien die Mitarbeiter angehört worden. Die sich als unbescholten erwiesenen Mitarbeiter habe man nicht informieren müssen, so Schaupensteiner: „Da haben wir keinen Anlass gesehen.“ Die gesammelten Daten seien ja schließlich wieder gelöscht worden. Dass auch LokomotivführerInnen oder ZugbegleiterInnen, die keine Aufträge vergeben, überprüft wurden, hänge mit der Methode zusammen.

Mehdorn informierte nach dem Bekanntwerden der Kontrollaktion von 1.000 Personen den Aufsichtsrat der Deutschen Bahn in einem Brief. Darin kam er zu dem Ergebnis, es könne „bereits heute mit Gewissheit gesagt werden, dass ein Vergleich mit den Datenschutzskandalen an anderer Stelle völlig unangemessen“ wäre. Nachdem dann das gesamte Ausmaß der Aktion bekannt wurde, äußerten er und Schaupensteiner sich am 30.01.2009 vor der Presse. Mehdorn verurteilte die „für uns nicht nachvollziehbaren, polemischen und überzogen dargestellten Vorwürfe“. „Wir haben in der Vergangenheit für unsere Arbeit bei der Korruptionsbekämpfung viel Lob von der Antikorruptionsorganisation Transparency International bekommen.“ Auch jetzt habe man sich nur an das gehalten, was von Wirtschaftsprüfern empfohlen werde. Es sei absolut üblich, dass Daten von Mitarbeitern mit denen von Lieferanten abgeglichen werden. Auf die Frage, ob die Empfehlung auch den heimlichen Abgleich erfasse, blieben Mehdorn und Schaupensteiner eine Antwort schuldig. Mehdorn schimpfte, bei Siemens habe man dem Ex-Vorstand vorgeworfen, zu wenig gegen Korruption getan zu haben: „Uns wirft man jetzt vor, dass wir zu viel getan haben.“ Um die Debatte zu versachlichen, habe der Konzern die Staatsanwaltschaft eingeschaltet: „Uns hört ja keiner zu; ich hoffe, Sie hören denen dann zu. Dies ist der weitestgehende Schritt, um Transparenz und Aufklärung zu schaffen. Wir erhoffen uns davon eine Versachlichung der Debatte und eine Besinnung auf die Fakten.“ Damit könne „einer unverantwortlichen Skandalisierung der Boden entzogen“ werden. Der Datenabgleich sei nichts weiter als ein „Screening“ gewesen. Von einer Rasterfahndung könne keine Rede sein. Auf die Frage, worin genau der Unterschied zwischen den Geschehnissen und einer Rasterfahndung liege, antwortete Schaupensteiner: „Googeln Sie das selbst nach“. Der Vorstand habe von dem Abgleich nichts gewusst, so Mehdorn: „Das hat damals die Innenrevision gemacht.“ Es sei „ganz normale Tagesarbeit“: „Der Vorstand kümmert sich ja auch nicht um die Bestellung von Briefcouverts“. Der Bahnchef verwahrte sich auch gegen die Einmischung von Bundesverkehrsminister Wolfgang Tiefensee (SPD): „Er hat damit nichts zu tun und braucht sich da auch nicht einzubringen.“

Wegen des öffentlichen Drucks beauftragte die Bahn eine externe Wirtschaftsprüfungsgesellschaft mit der Überprüfung der Kontroll-Methoden. Zudem erklärte der Bahn-Chef, den Dialog mit Betriebsräten zu suchen, die sich zuvor entsetzt über das Ausmaß der Bespitzelungen gezeigt hatten. Er kündigte intensive Gespräche mit den Arbeitnehmervertretern an, „um zukünftig Einiges zu verbessern“. Das Unternehmen teilte ergänzend mit, dass bis 2007 nach den Überwachungsmaßnahmen insgesamt 543 konkreten Verdachtsfällen nachgegangen worden sei, wovon 148 zu strafrechtlichen Ermittlungsverfahren geführt hätten. Die DB habe rund 30 Mio. Euro Rückzahlungen aus Korruptionsschäden verbuchen können.

Bahn-Sprecher Schumacher: „Dabei ging es keineswegs nur um millionenschwere Verfehlungen auf der Ebene von Führungskräften, sondern weit darunter auch um kleinere Fälle im Bereich der Gebäudereinigung und des Grünschnitts entlang den Gleisen.“ Einige Bahn-Mitarbeiter und Geschäftspartner seien daraufhin in Strafverfahren „zu hohen Haftstrafen“ verurteilt worden.

Tiefensee forderte eine schnelle und umfassende Aufklärung der Datenaffäre. Neue Tatsachen dürften nicht scheibchenweise an die Öffentlichkeit gelangen: „Wenn die Bahn sich im Rahmen der Korruptionsbekämpfung, die zweifellos eine wichtige Aufgabe ist, korrekt verhalten hat, dann kann dies ja schnell und umfassend dargelegt werden.“ Kanzlerin Angela Merkel verlangte eine „lückenlose“ Aufklärung. Der Verkehrsausschuss des Bundestags hat einen Katalog mit 119 zu beantwortenden Fragen an die Bahn erarbeitet. Die grünen Bundestagsabgeordneten Winfried Hermann und Anton Hofreiter sprachen von einem Massendatenabgleich: „Mit dieser heimlichen Ausspähung in großem Stile stellt die Bahn AG alle Mitarbeiter und Mitarbeiterinnen unter Generalverdacht und verstößt massiv gegen deren schutzwürdige Interessen.“ Deren Kollegin Silke Stokar hielt bei dem Vorgehen der Bahn vor allem für bedenklich, dass „die innere Sicherheit privatisiert“ werde. Auch der Aufsichtsrat machte Druck. Aus dem Umfeld des Kontrollgremiums war zu hören, die Stimmung sei dort nicht mehr unbedingt „pro Mehdorn“, sondern eher gereizt. Die Gewerkschaften Transnet und GDBA forderten ebenfalls Konsequenzen bei der Bahn. Die Bahn-Mitarbeiter hätten ein Anrecht auf umfassende, nicht scheibchenweise Aufklärung. So „richtig und wichtig“ der Kampf gegen Korruption sei, so dürfe die Bahn mit der präventiven Kontrolle nicht Grenzen überschreiten. Der Bahn-Aufsichtsrat oder andere Gremien müssten Kontrollaktionen überwachen. Der BlnBDI Dix teilte dem Bundestag mit, er werde seine Prüfung spätestens in einem halben Jahr abschließen (Gatzke/Güßgen/Röhrig www.stern.de 21.01.2009; PI DB Mobility Networks Logistics 21.01.2009; www.spiegel.de 21.01.2009; Bauchmüller SZ 22.01.2009, 17; Schwenn www.faz.net 21.01.2009; Kazim/Seith www.spiegel.de 21.01.2009; Dohmen/Schmitt Der Spiegel 5/2009, 68 f.; www.spiegel.de 28.01.2009; Leyendecker, Bauschmüller/Ott SZ 30.01.2009, 4, 6; www.heise.de 30.01.2009; Haustein-Teßner www.welt.de 30.01.2009; Kuhr/Ott SZ 31.01./01.02.2009, 25).

Bund

Erweitertes Führungszeugnis soll Kinder vor Pädophilen schützen

Bundesjustizministerin Brigitte Zypries lässt in ihrem Haus einen Gesetzentwurf vorbereiten, der ein „erweitertes Führungszeugnis“ vorsieht. Dieses soll ermöglichen, diejenigen genauer zu überprüfen, die mit Kindern und Jugendlichen arbeiten. Bisher, so Zypries, „können sich Menschen mit pädophilen Neigungen ganz gezielt Arbeitsfelder mit Kontakten zu Kindern und Jugendlichen suchen“. Das derzeit übliche Führungszeugnis, das jeder Arbeitgeber von einem Bewerber für eine Stelle verlangen kann, listet nur Freiheitsstrafen von mehr als 90 Tagessätzen auf. Weniger schwere Delikte werden nicht aufgeführt. Seit 1998 gibt es die Ergänzung, dass bei schweren Sexualdelikten wie sexuellem Missbrauch oder Vergewaltigung eine Aufnahme auch dann erfolgt, wenn die vom Gericht verhängte Strafe geringer ist. Der Handel mit kinderpornografischen Bildern, der in den letzten Jahren zu Hunderten Strafverfahren und Schuldsprüchen geführt hat, zählt bisher nicht dazu. Das „erweiterte Führungszeugnis“ soll dies ändern. Das neue Zeugnis soll nur an Menschen ausgegeben werden, die beruflich häufig mit Kindern zu tun haben. Dazu zählen nach den ministeriellen Plänen ErzieherInnen, MitarbeiterInnen der Jugendämter, SporttrainerInnen und BademeisterInnen. Der im Januar 2009 im Bundeskabinett beratene Gesetzentwurf wird von den Bundesländern unterstützt. Der Journalist Manfred Karremann, der ein Jahr lang verdeckt in der Szene der Pädophilen recherchiert hat, geht davon aus, dass das neue Gesetz für Unruhe sorgen wird: „Die Pädophilen diskutieren jede Gesetzesänderung akribisch.“ Er könne sich vorstellen, dass Einzelne klar erkennen, dass sie mit einem „erweiterten Führungszeugnis“ keine Chance auf manche Jobs in der Nähe von Kindern hätten und sich deshalb gar nicht bewerben würden (Berth SZ 27.11.2008, 1).

Bund

Lidl und Bildzeitung gemeinsam für „Leserreporter“

Kurz vor Weihnachten 2008 brachte der Discounter Lidl Camcorder in seine Läden, mit deren Hilfe „Bild“-Leserreporter ihre Filme per Knopfdruck direkt an die Springer-Redaktion senden können. Der Camcorder „Creative Vado“ kostet 69,99 Euro und sendet per Knopfdruck Videos in die Redaktion der Boulevard-Zeitung. Der Discounter und die Zeitung warben in einer Pressemitteilung mit dem günstigen Angebot: „Vergleichbare Geräte kosten ca. 100 Euro im Handel“. Tatsächlich war das Gerät aber - ohne Software für die Direktschalte ins Axel-Springer-Haus - im Internet aber bereits für 78,98 Euro zu haben. Sprecher der Bild, Thomas Fröhlich: „Die Kamera hat vier Knöpfe. Sie macht es kinderleicht, Leser-Reporter zu werden.“ Was für die Zeitung ein Verkaufsargument ist, scheint Lidl zur Verteidigung zu veranlassen, zumal die März 2008 bekannt gewordene Videobespitzelung in Lidl-Filialen noch in Erinnerung ist, so Simone Hartmann: „Der Umgang und die Verwendung mit diesem Produkt liegen allein beim Kunden.“ Der Camcorder sei nur „ein attraktives Angebot vor Weihnachten.“ Der Deutsche Journalistenverband (DJV) fand die Aktion bedenklich, so Hendrik Zörner: „Laien kennen keinen Medienkodex. Wenn sie sich nicht benehmen, muss demnächst ein Journalist draußen bleiben“. Bei der Bildzeitung wird derweil beraten, wie Hobbyjournalismus noch weiter ge-

fördert werden kann, so Fröhlich: „Für die Reporter ist ein Anreiz geplant“ (zu Leserreporter vgl. DANA 4/2006, 171; Kühn, www.taz.de 04.12.2008).

Bund

Schaar wiedergewählt

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Peter Schaar bleibt für weitere 5 Jahre im Amt. Der Bundestag wählte den 54-jährigen studierten Volkswirt am 26.11.2008 mit 484 zu 52 Stimmen bei 12 Enthaltungen. 6 Stimmen waren ungültig. Schaar, der die Funktion Ende 2003 auf Vorschlag der Grünen als Datenschutzbeauftragter übernommen hatte, war von der Bundesregierung für eine weitere Amtszeit vorgeschlagen worden. 2003 hatte Schaar lediglich 347 Stimmen bekommen, bei 227 Gegenstimmen. 2006 kam die Informationsfreiheit als Aufgabe hinzu. Schaar war Gründungsmitglied der Grün-Alternativen Liste in Hamburg und dort von 1997 bis 2000 Vorstandssprecher. Vor seiner Wahl zum Datenschutzbeauftragten des Bundes war er Stellvertreter des Hamburgischen Datenschutzbeauftragten. Eine weitere Verlängerung der Amtszeit über 2012 hinaus ist nicht mehr möglich (SZ 27.11.2008, 6; Welt Kompakt 27.11.2008, 5; FR 27.11.2008, 6; Krempl, www.heise.de 26.11.2008).

Bund

BND überwacht Telekommunikation von Entwicklungshelfern

Der deutsche Auslandsgeheimdienst BND (Bundesnachrichtendienst) hat jahrelang ein Büro der Deutschen Welthungerhilfe in Afghanistan überwacht. Von Oktober 2005 bis April 2008 wurde der E-Mail-Verkehr des von der Welthungerhilfe geleiteten Afghanistan NGO Safety Office (Anso) teilweise mitgelesen. Die Abhöraktion sei „zur Erkennung und Begegnung internationaler terroristischer Anschläge“ durchgeführt worden, die Auswertung der Informationen habe der „Einschätzung der allgemeinen Sicherheitslage in Afghanistan“ und dem Schutz deutscher Einrichtungen gedient, wurde gegenüber den Entwicklungshelfern vom BND mitgeteilt. Zur Zeit der Überwachung wurde die Welthungerhilfe von Ingeborg Schäuble geleitet, der Ehefrau des Bundesinnenministers. Das Anso ist ein gemeinsames Büro westlicher Nichtregierungsorganisationen in Kabul und bündelt die Erkenntnisse der Hilfsorganisationen. Die Stelle unterhält Außenbüros in vier afghanischen Provinzen, finanziert wird sie von der Europäischen Union. Das Netzwerk sei ein „Seismograph“ der Entwicklung am Hindukusch, heißt es bei der Welthungerhilfe. Der BND wollte offenbar von diesem internen Wissen möglichst frühzeitig und umfangreich profitieren. Die zuständige Abteilung des BND in Pullach zeichnete mindestens 2000 Telefonate, Emails und Faxe auf. Inzwischen erkennt auch der BND an, dass die Kommunikation in Kabul „grundrechtlich geschützt“ ist. Es wird geprüft, ob die Abhöraktion rechtswidrig war. Der Generalsekretär der Deutschen Welthungerhilfe, Hans-Joachim Preuß, forderte Bundeskanzlerin Angela Merkel (CDU) auf, den Vorfall zu untersuchen und sicherzustellen, dass Entwicklungshelfende nicht mehr abgehört werden (Der Spiegel 50/2008, 17; SZ 09.12.2008, 6).

Bund

Wikilead fühlt sich von BND verfolgt

Der anonymen Plattform für regierungskritische Veröffentlichungen Wikileak wurde nach Mitteilung auf deren Webseite vom Chef des deutschen Bundesnachrichtendienstes (BND), Ernst Uhrlau, mit unmittelbaren rechtlichen Schritten gedroht, wenn sie nicht ihre Artikel über den BND entfernt. Wikileak hatte zuletzt einen Artikel des Journalisten Tom Burghardt veröffentlicht, in dem dieser behauptet, die drei im Zusammenhang mit einem Bomben-Attentat festgenommenen BND-Mitarbeiter hätten einen Laptop bei sich gehabt, durch dessen Beschlagnahme die Namen ihrer Informanten in die Hände des als korrupt geltenden Kosovo-Regimes gelangt seien. Außerdem gehe es um Artikel über den Schäfer-Bericht (vgl. DANA 2/2006, 83 f.) und Manipulationen seitens des BND im Internet. Wikileak ist eine Webseite, auf der grds. jedeR ungeprüft und anonym Beiträge einstellen kann. Sie orientiert sich an Wikipedia und grenzt sich von Whistleblowern ab: „Wikileak führt keinerlei Prüfung der auf ihrer Homepage veröffentlichten Dokumente durch, wodurch deren Echtheit nicht gesichert ist.“ Im Frühjahr 2008 wurde Wikileak wegen der Veröffentlichung interner Bankdaten von der Schweizer Bankengruppe Julius Bär verklagt, die ihre Klage aber kurz darauf wieder zurückzog (www.heise.de 21.12.2008).

Bund

BKA hält Datenschutzbeauftragten geheim

In Entwürfen des inzwischen ohne diese Regelung in Kraft getretenen Bundeskriminalamtsgesetzes (BKAG) war vorgesehen, dass der behördliche Datenschutzbeauftragte des BKA für die Sicherung des Kernbereichs privater Lebensgestaltung bei verdeckten Ermittlungsmaßnahmen (Online-Durchsuchung) zuständig sein sollte. Dies veranlasste Journalisten zu recherchieren, wer diese Aufgabe tatsächlich wahrnimmt. Sie mussten dabei feststellen, dass das BKA diesen Namen geheim hält: „Wir machen die Namen von BKA-Bediensteten grundsätzlich nicht öffentlich.“ Verraten wurde nur soviel: Der Mann arbeitet seit 1993 für das BKA und ist Jurist. Datenschutzbeauftragter ist er seit November 2007. Vorher war er Dozent für Staats- und Verfassungsrecht an der Fachhochschule des Bundes. Für seine Aufgabenwahrnehmung stehen ihm vier MitarbeiterInnen zur Verfügung. Die taz bezweifelte – wohl nicht ganz zu Unrecht – die Vertrauenswürdigkeit eines namentlich geheim gehaltenen Datenschutzbeauftragten für die von der

Datenverarbeitung Betroffenen (Rath www.taz.de 16.12.2008; zum BKAG Hülsmann, S. 16 ff.).

Bund

Schufa sammelt Auskunftsverlangen an Auskunfteien

Vom 15.01.2009 an können sich VerbraucherInnen bei der Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) darüber informieren, welche persönlichen Daten nebst Scorewert nicht nur dort, sondern auch bei fünf weiteren Auskunfteien gespeichert sind. Bei den fünf Unternehmen handelt es sich um accumio finance services (Deutsche Telekom), arvato infoscore (Bertelsmann), Bürgel Wirtschaftsinformationen (Allianz), CEG Creditreform Consumer (Neuss) und Deltavista (München, Schweiz). Das Quintett gehört bundesweit zu den größten Auskunfteien. Diese sammeln Informationen zur Bewertung der Zahlungsmoral (Bonität) von KundInnen und beauskunften diese Angaben oder Zusammenfassungen in Scorewerten an anfragende Unternehmen. Schon bisher können registrierte InteressentInnen ihre bei der Schufa gespeicherten Daten über die Webseite „meineschufa.de“ online einsehen oder als Eigenauskunft bestellen. Mit dem neuen Service können sie nun auch herausfinden, was bei den anderen fünf gespeichert ist. Die NutzerIn fordert über die Schufa bei den Unternehmen ihre Eigenauskunft an. Das Formular wird an die jeweiligen Auskunfteien weitergeleitet. Diese schicken die Auskünfte dann per Post an die VerbraucherIn, ohne dass die Schufa auf die Daten zugreifen kann. Angeboten wird der Service aber nur für angemeldete Nutzende des Internetportals der Schufa, die sich einmalig für 15,60 Euro registrieren lassen müssen. Das 2005 eingerichtete Portal der Schufa zählt derzeit mehr als 400.000 registrierte NutzerInnen.

Schufa-Chef Rainer Neumann erklärt: „Wir wollen den Verbrauchern einen Überblick verschaffen, welche Firmen außer der Schufa ihre kreditrelevanten Daten gespeichert haben könnten.“ Insgesamt gibt es etwa 60 Auskunfteien in Deutschland. Bei Creditreform kostet die Auskunft an die Betroffenen pro Person 7,60 Euro; bei den anderen ist das Angebot kostenlos. Christina Beck von der Verbraucherzentrale Bundesverband (vzbv) kritisiert: „Das ist eine Art Nebelkerzenwerfen, nach dem Motto, wir tun doch etwas“. Wichtiger für eine echte Transparenz sei es, dass die Schufa ihre Kundenbewertungskriterien offenlege. Solange dies nicht der Fall sei, „sehen wir dieses Vorhaben eher skeptisch“. Hintergrund der Auskunfteieninitiative ist offensichtlich die derzeitig erfolgende Überarbeitung des Bundesdatenschutzgesetzes (BDSG), die von den Auskunfteien bisher heftig bekämpft wurde. Danach müssen VerbraucherInnen künftig besser informiert werden, welche Auskunftei welche Daten und welche Scores über sie gespeichert hat. Nun fordert Neumann eine Verschärfung des geplanten Gesetzes, da nach wie vor für die Betroffenen unklar bleibe, welche Unternehmen Daten zu ihrer Person speichern und weitergeben dürfen. Er setzt sich daher für ein Zulassungsverfahren für Auskunfteien ein.

Silke Stokar, innenpolitische Sprecherin der Grünen im Bundestag, begrüßte den Vorstoß der Schufa als „Schritt in die richtige Richtung“. Damit würden große Akteure im Auskunfteienbereich „unabhängig von dem Reförmchen der großen Koalition“ in einem Verbund mehr Transparenz schaffen. Erforderlich sei aber eine gesetzliche Verpflichtung aller Scoring-Anbieter, über ein unabhängiges, kostenloses Verbraucherportal den Betroffenen die Möglichkeit zur Abfrage der über sie gespeicherten Daten und Werte zu geben. Weiter müssten die Kunden der Auskunfteien etwa im Versandhandel, im Finanzsektor oder im Telekommunikationsmarkt angehalten werden, die Verbraucher auf ihren Webseiten darüber zu informieren, mit welchen Scoring-Firmen sie zusammenarbeiten. Sie wolle persönlich wissen, welche Auskunftei etwa Quelle.de oder Otto.de mit einer Bonitätsprüfung beauftrage (von Kempis SZ 15.01.2009, 25; Krempl www.heise.de 14.01.2009; Panitz www.welt.de 14.01.2009).

Bund

Payback übermittelt Kundendaten an Real

KassiererInnen der Handelskette Real haben ihre eigenen Payback-Karten genutzt und damit Punkte von KundInnen ohne eigene Kundenkarte gesammelt. Um diesen „Missbrauch“ des Payback-Systems aufzuklären, hat der Rabattanbieter die Nutzungsdaten an den Real-Konzern weitergegeben; dieser feuerte die MitarbeiterInnen. Betriebsräte von Real-Filialen in Deutschland bestätigten, dass in den letzten zwei Jahren KollegInnen ihren Job verloren, nachdem sie ihre Payback-Karte während der Arbeitszeit nutzten. Real spricht von einer niedrigen zweistelligen Zahl von Kündigungen. Die Real-Angestellten hatten offenbar Rabatte von fremden KundInnen auf einem eigenen Payback-Konto verbucht, zumindest teilweise auch in Absprache mit dem KäuferInnen. Wie bei sonstigen KundInnen auch, geben die Belege der Rabattbuchungen von Payback keinen Namen preis, sondern nur die Kartennummer. Insbesondere, wenn Real die Payback-Karte nicht selbst ausgegeben hat, sondern ein anderes Partnerunternehmen, wie z.B. die Tankstellenkette Aral oder der Drogeriemarkt DM, haben die Verantwortlichen keinen Zugriff auf die persönlichen Daten der Inhaber. Payback versichert in seinem „Hinweis zum Datenschutz“: „Jede Möglichkeit einer Identifizierung Ihrer Person durch Partnerunternehmen oder Dritte ist ausgeschlossen.“

Im Widerspruch hierzu gab es eine Kooperation zwischen Real und Payback; an beiden Unternehmen ist der Handelskonzern Metro beteiligt. Real behauptet, es habe damit auf Kundenbeschwerden reagiert. Kassenprotokolle wurden auf auffällige Payback-Transaktionen hin überprüft. Wurden in kürzeren Zeiträumen an derselben Kasse wiederholt Punkte auf das gleiche Payback-Konto gebucht, informierte der jeweilige Marktleiter die interne Revision. Real nahm Kontakt zu Payback auf: „Wenn sich der Verdacht bestätigt, dass hier möglicherweise Straftaten zum Nachteil dritter Kunden

oder des Unternehmens begangen worden sind, fordert er die Personendaten zum entsprechenden Konto an." Payback spricht von „absoluten Ausnahmen". Bei hinreichendem Verdacht, dass eine Straftat wie Unterschlagung oder Veruntreuung vorläge, mache man Real Namen und Anschrift des Betroffenen zugänglich. Nach § 28 Bundesdatenschutzgesetz (BDSG) sei die Weitergabe erlaubt, wenn sie der Verfolgung einer Straftat dient. Im Fall Real gehe es um „Straftatbestände" und nicht etwa um „vage Verdachtsmomente und Kavaliersdelikte".

Der Datenschutzbeauftragte von Schleswig-Holstein, Thilo Weichert, kritisiert die Payback-Real-Kooperation: „Die Datenlieferung ist unzulässig. Ich kann keine der von Payback geschilderten Straftatbestände nachvollziehen." Tatsächlich erklärt Real, dass gegen die betroffenen MitarbeiterInnen keine zivilrechtlichen Schritte unternommen wurden und auch keine Strafanzeigen gestellt wurden, weil der Schaden in den meisten Fällen zu gering gewesen sei. Weichert weist darauf hin, dass die Preisgabe von Informationen bei Straftatverdacht nicht ausreichend in den Nutzungsbedingungen thematisiert wird: „Bei Straftatverdacht dürfte nicht der Arbeitgeber informiert werden, sondern die Staatsanwaltschaft. Will Payback sich auf § 28 berufen, muss hierauf ausdrücklich hingewiesen werden. Payback ist bei der Kooperation mit Real gegenüber den Kunden wortbrüchig geworden."

Payback kontert: „Die Hinweise können und wollen nicht jeden Ausnahmefall - und um einen solchen handelt es sich ja vorliegend - beschreiben." Zudem seien Datenschutzhinweise nicht dazu da, potenzielle Straftäter auf die geltenden Bestimmungen im Strafgesetzbuch oder dem BDSG hinzuweisen oder diese Personen darüber aufzuklären, was im Falle von Betrug oder Unterschlagung geschehen kann. Dies überzeugt Weichert nicht: „Payback verstößt bei der Datenweitergabe gegen Datenschutzrecht." Aus seiner Sicht beschränkt sich der Missstand dabei nicht auf die Zusammenarbeit mit Real. „Jeder Payback-Kunde muss theoretisch damit rechnen, dass das Unternehmen persönliche Daten ohne Absprache weitergibt - auch wenn es dafür eigentlich keine ausreichende Gründe gibt" (Hauser/Sucher www.spiegel.de 05.12.2008).

Bund

Zweifelhafte Mieter-Warndatei

Die Firma Die.wa.da GmbH aus Bergheim verspricht VermieterInnen Auskunft über Zuverlässigkeit und Unbescholtenheit von MietbewerberInnen. In der Internet-Warndatei sollen relevante Informationen über WohnungsinteressentInnen abgerufen werden können, z.B. wenn gegen eine MieterIn ein Urteil zu einer fristlosen Kündigung wegen Mietrückständen oder vertragswidrigem Verhalten oder ein Haftbefehl vorliegt. Zwei Anfragen kosten 35,70 Euro. Firmensprecherin Marie Luise Erdell will keine Aussage machen, wie viele Datensätze verfügbar sind, so dass VermieterInnen nicht abschätzen können, ob sich eine Abfrage überhaupt lohnt. Misstrauisch machen auch Angaben auf der Internetseite der Firma über einen angeblichen Unternehmensbeirat. Einer der als Mitglied des Beirats aufgeführten Anwälte erklärte gegenüber Finanztest, diesem Gremium nicht anzugehören. Finanztest gibt VermieterInnen den Ratschlag, bei dem Verdacht, es mit einem „Mietnomaden" zu tun zu haben, sich in den öffentlichen Schuldnerverzeichnissen bei den Amtsgerichten zu informieren. Eine Nachfrage beim Gericht des vorherigen Wohnortes der InteressentIn offenbart, ob diese in den vergangenen drei Jahren dort eine eidesstattliche Versicherung abgegeben hat, gegen sie ein Haftbefehl ergangen ist oder ein Insolvenzverfahren mangels Vermögens nicht eröffnet werden konnte (Finanztest 12/2008, 42).

Nordländer/Bund

Übergreifende Abhörzentralen geplant

Die Innenminister und -senatoren der norddeutschen Bundesländer Niedersachsen, Bremen, Hamburg, Schleswig-Holstein und Mecklenburg-Vorpommern haben sich am 24.11.2008 in Bremen auf der Innenministerkonferenz Nord (IMK-Nord) darauf verständigt, bei Polizei- und Verfassungsschutzaufgaben enger zusammenzuarbeiten. Die Leiter der Polizeiabteilungen wurden beauftragt zu prüfen, ob und in welchen Bereichen der kriminaltechnischen Untersuchungsstellen (KTU) künftig eine gemeinsame Aufgabenerledigung sinnvoll ist. Erörtert wurde auch ein Bericht der gemeinsamen Arbeitsgruppe von Polizei und Verfassungsschutz zur Bildung eines regionalen Verbundzentrums zur Telekommunikationsüberwachung (TKÜ). Die fünf Länder könnten sich dadurch die Kosten für teure TKÜ-Technik teilen und müssten nicht alle einzeln anschaffen, erklärte Niedersachsens Innenminister Uwe Schünemann (CDU). Die Prüfung der Kooperation und Zentralisierung bei der TKÜ und von Operativtechnik soll bis zum Sommer 2009 abgeschlossen werden.

Die Prüfung der Bündelung der TKÜ steht im Kontext der Pläne des Bundesinnenministeriums (BMI) seit Sommer 2008, wonach Abhörtechnik künftig gemeinsam vom Bundesamt für Verfassungsschutz, der Bundespolizei und dem Bundeskriminalamt (BKA) genutzt werden soll. Hierfür soll ein technisches Servicezentrum und eine Art übergeordnete Denkfabrik entstehen. Beim Bundesrechnungshof stieß die von Kritikern als „Bundesabhörzentrale" bezeichnete Einrichtung auf Ablehnung, da es Kostenvorteile durch die Umstrukturierung für den Zeitraum bis 2015 nicht gebe. Auch sei die Wahl des Bundesverwaltungsamtes (BVA) als Standort der neuen Einrichtung „nicht nachvollziehbar". Der Rechnungshof empfiehlt vielmehr ein „Zwei-Säulen-Modell" - ein gemeinsames Rechenzentrum der Polizeien beim Bundeskriminalamt und ein Rechenzentrum für die Verfassungsschützer aus Bund und Ländern beim Bundesamt für Verfassungsschutz in Köln (www.heise.de 24.11.2008).

Baden-Württemberg

Routine-Erhebung von genetischem Fingerabdruck bei Straßenkontrollen

Im Landkreis Ludwigsburg gehört seit Sommer 2008 neben der Überprüfung von Führerschein und Kfz-Papieren die Abnahme des genetischen Fingerabdrucks bei Fahrzeugkontrollen zur Routine. Betroffen sind Männer und Frauen. Die Polizei begründet ihre Versuche, AutofahrerInnen zur freiwilligen Abgabe von Speichelproben zu bewegen, mit der Fahndung nach der Phantommörderin von Heilbronn. Die Betroffenen geben oft ihre Einwilligung nur, weil sie sich unter Druck gesetzt fühlen, z.B. wenn sie bei der Straßenkontrolle irrtümlich falscher Adressangaben bezichtigt werden. Die Polizeidirektion Ludwigsburg dagegen behauptet, niemand werde von der Polizei zum Mitmachen bei einem DNA-Test gedrängt; die Abnahme erfolge freiwillig und unter strikter Wahrung der rechtlichen Bestimmungen. Die Routinekontrollen werden damit begründet, dass die Polizistenmörderin von der Heilbronner Theresienwiese auch im Landkreis ihren genetischen Fingerabdruck hinterlassen habe, nämlich in Gronau und Kornwestheim. Bei normalen Kontrollen würden daher auffällige Personen verstärkt um die Abgabe der Speichelprobe gebeten. Sollte der DNA-Test negativ verlaufen, werde die Probe umgehend vernichtet. Die Daten der Überprüften blieben hingegen zeitweise in einer Negativdatei gespeichert, was vom Heilbronner Polizeisprecher begründet wird: „Sie sind dann bei einer möglichen abermaligen Kontrolle außen vor.“ Wie viele Verkehrsteilnehmer bisher „sicherheitsgenetisch behandelt“ wurden, kann die Polizeidirektion Ludwigsburg nach eigenen Angaben nicht sagen, weil ja die Proben vernichtet würden. Wann eine Genprobe erbeten wird, so die Angaben aus Heilbronn, sei „weitgehend eine Sache des Näschens unserer Kollegen“. Es gebe Kriterien, „über die wir nur teilweise offen reden können“. Es sei bekannt, dass die mehrfache Mörderin äußerlich möglicherweise gar nicht als Frau identifizierbar ist, häufiger in Gartenhäuschen nächtige, weshalb man sie „nicht unbedingt in einem Nadelstreifenanzug“ antreffen werde. Auch Landfahrer und Schausteller habe man wegen des Tatortes Theresienwiese verstärkt im Auge. Bei zielgerichteten und damit nicht „nebenher“ am Straßenrand gezogenen DNA-Proben wurden im Kreis Ludwigsburg im Jahr 2008 bis Anfang Dezember 289 Personen überprüft. Im Jahr 2007 waren es insgesamt 304 Personen. Insgesamt seien in den Landkreisen Ludwigsburg und Heilbronn bei routinemäßigen Polizeikontrollen auf freiwilliger Basis ca. 1.300 DNA-Checks durchgeführt worden (Pross, www.ludwigsburger-kreiszeitung.de 10.01.2009; Krempl www.heise.de 12.01.2009).

Baden-Württemberg

Daimler speichert unzulässig Daten über kranke MitarbeiterInnen

Die Datenschutzaufsichtsbehörde Baden-Württemberg, das dortige Innenministerium, rügte den Autobauer Daimler wegen des Umgangs mit Informationen über kranke MitarbeiterInnen. Über MitarbeiterInnen des Werks Untertürkheim, die länger krank waren, wurden unzulässige Daten z.B. über Diagnosen oder Krankheitsursachen erhoben. Die Betroffenen wurden nicht informiert, was mit den Daten passiert. Eine Daimler-Sprecherin kündigte eine Änderung der Praxis an. Es sei mit dem Prüfbericht nun Rechtsklarheit zur Gestaltung des Gesundheits- und Fehlzeitenmanagements geschaffen worden. Die geforderten Anpassungen würden vorgenommen, um den Datenschutz seiner Beschäftigten im vollen Umfang zu gewährleisten. Es handele sich nicht um einen „Datenschutzskandal“. Das Verfahren sei schließlich nicht in Frage gestellt worden. Die Ermittlungen des Innenministeriums gingen auf Beschwerden einer „Betriebsratsminderheit“ im Werk Untertürkheim zurück. Das Gesundheitsmanagement von Daimler sieht verschiedene Formen von Mitarbeitergesprächen nach Abwesenheiten vor, insbesondere bei mehrfachen oder längeren Erkrankungen. Darüber hinaus gibt es einen Runden Tisch, an dem die Führungskräfte einer Abteilung, Vertreter der Personalabteilung, des werkärztlichen Dienstes und des zuständigen Bereichs-Betriebsrats Fälle mit hohen Fehlzeiten und sonstige auffällige Fälle erörterten. Ziel sei es, Fehlzeiten zu reduzieren und Beschäftigte nach einer Krankheit wieder zu integrieren. Das Innenministerium kritisierte, dass an den Gesprächen am Runden Tisch Personen teilgenommen haben, die nicht oder nur zeitweise hätten teilnehmen dürfen, z.B. Meister, die nicht Vorgesetzte der betroffenen MitarbeiterIn sind und für deren Anwesenheit es auch sonst keinen zwingenden Grund gab, der Werksarzt oder der Vertreter des Bereichs-Betriebsrats (SZ 07.01.2009, 19).

Bayern

Thomas Petri neuer Landesbeauftragter für Datenschutz

Die Bayerische Staatsregierung hat auf ihrer Kabinettssitzung am 20.01.2009 den derzeitigen Stellvertreter des Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) Dr. Thomas Petri als neuen Landesbeauftragten für den Datenschutz (BayLfD) vorgeschlagen. Petri war nach dem 2. juristischen Staatsexamen zunächst als Rechtsanwalt tätig. Danach war er u.a. wissenschaftlicher Mitarbeiter an der Universität Frankfurt, Lehrstuhl für öffentliches Recht und Rechtsphilosophie, Leiter des Referats Privatwirtschaft im Unabhängigen Landeszentrum für Datenschutz in Kiel sowie wissenschaftlicher Mitarbeiter am Bundesverfassungsgericht. Seit dem 01.07.2006 ist er Stellvertreter des BlnBDI im Bereich Recht. Petri soll dem bisherigen BayLfD Dr. Karl-Michael

Betzl nachfolgen, der im Oktober 2008 auf seine Bitte hin vom damaligen Landtagspräsidenten Alois Glück von seinem Amt wegen Ermittlungen wegen Steuerhinterziehung entbunden worden war (DANA 2/2008, 78 f.). Das Amt des BayLfD wird auf die Dauer von 6 Jahren ausgeübt. Die Ernennung erfolgt durch den Präsidenten des Bayerischen Landtags. Petri hat bei seiner Vorstellung die möglichen Interessenkollisionen angesprochen, die es zwischen dem Datenschutz und anderen Behörden gebe, berichtete Bayerns Innenminister Joachim Herrmann. Von geringem Selbstbewusstsein sei der Neue nicht. Dies bestätigte Petri. Er werde sich sicher mit dem Innenminister auseinandersetzen, aber auch zusammensetzen: „Ich bin nicht rot, nicht schwarz, nicht grün, nicht lila. Ich bin ein Fachmann, kein Politiker“ (www.bayern.de 20.01.2009; SZ 21.09.2009, 31; Ramelsberger SZ 22.01.2009, 4).

Bayern

Funkzelleninformations-system ortet Handys punktgenau

Das bayerische Innenministerium stellte der Öffentlichkeit am 01.12.2008 ein System zur Ortung von Mobiltelefonen vor, das bis auf wenige Meter genau arbeiten soll. Das vom Landeskriminalamt (LKA) und Wissenschaftlern entwickelte „Datenbank Funkzelleninformationssystem“ (FIS-Bayern) kombiniert GPS-Daten mit Funkzellenmessungen und soll vor allem bei der Bergung von Unfallopfern in entlegenen Gebieten oder bei der Suche nach Vermissten helfen. Bisher konnte die Polizei Mobiltelefone nur funkzellengenau lokalisieren, was im ländlichen Raum oft eine Fläche von mehreren Quadratkilometern umfasst. Um genauere Daten zu erhalten, werden 20 Streifenwagen mit Messinstrumenten ausgerüstet, die während der Dienstfahrten GPS-Daten, Funkzellen-IDs und Signalstärken in den Funkzellen protokollieren. Im Gebirge tragen alpine Einsatzkräfte die Geräte im Rucksack. Die Daten werden in der Einsatzzentrale miteinander verknüpft. Seit Mitte 2007 sind ca. 70-75% des Freistaates im System erfasst. Liegt dem LKA eine „Unglücksvermutung von einem Dritten“, z.B. eine Vermisstenanzeige von Angehörigen, vor, so übermittelt der Mobilfunkbetreiber die Funkdaten der letzten Verbindung zwischen Handy und Funkzelle. Diese Informationen gleicht die Polizei mit dem Informationssystem ab und kann so die Position des Handys bis auf wenige Meter genau bestimmen. Als Anwendungsfall nannte der Sprecher des Innenministeriums Holger Plank einen verunglückten Radfahrer, der mit Hilfe des Ortungssystems innerhalb einer halben Stunde habe geborgen werden können. Eine Ausweitung des Systems auf andere Bundesländer ist nach Angaben des bayerischen Innenministeriums bisher nicht angedacht. Auch für einen Einsatz in anderen Bereichen, z.B. der Verbrechensbekämpfung, gäbe es noch keine Pläne, so Plank: „So weit sind wir nicht“ (www.heise.de 01.12.2008).

Bayern

CSU will Verdächtigenherkunft für Kriminalstatistik

Die CSU will neben der Staatsangehörigkeit auch die Herkunft von Tatverdächtigen in der Kriminalstatistik erfassen. CSU-Landesgruppenchef im Bundestag Peter Ramsauer erklärt: „Die Abnahme der Ausländerkriminalität, die immer behauptet wird, ist vor allem dadurch herbeigeführt worden, dass Ausländer durch die Zuerkennung der deutschen Staatsangehörigkeit formal Deutsche geworden sind. So sinkt statistisch natürlich die Ausländerkriminalität.“ Der bayerische Innenminister Joachim Herrmann ergänzt: „Differenzierte Daten zur Straffälligkeit einzelner Bevölkerungsgruppen sind für eine wirksame Kriminalitätsbekämpfung wichtig. Mit der Änderung des Staatsangehörigkeitsrechts zum Jahr 2000 wurde der Zugang zur deutschen Staatsbürgerschaft erheblich erleichtert. Gerade junge Menschen haben von den verbesserten Einbürgerungsmöglichkeiten Gebrauch gemacht. Sie zählen damit zur deutschen Bevölkerung, haben aber einen Migrationshintergrund. Ähnliches gilt für Aussiedler, die die deutsche Staatsangehörigkeit Kraft Gesetz haben.“ Herrmann hat sich in einem Telefonat mit Hamburgs Innensenator Christoph Ahlhaus darauf geeinigt, eine gemeinsame Arbeitsgruppe einzurichten, in der Details für die praktische Umsetzung der Datenerhebung erarbeitet werden sollen. SPD-Innenpolitiker kritisierten, dass der Begriff „Zuwanderungshintergrund“ kaum sinnvoll zu definieren sei. Unklar sei, bis in welche Generation zurückverfolgt werden solle. Der innenpolitische Sprecher der SPD-Fraktion Sebastian Edathy sprach von „rechtspopulistischer Schaumschlägerei“, die in „Bürger erster und zweiter Klasse“ unterteile. Unterstützer des CSU-Vorstoßes beklagten dagegen, SPD und Grüne behandelten den Wunsch nach Erkenntnisgewinn wie ein Verbrechen. Der Vorsitzende der Deutschen Polizeigewerkschaft (DPolG) Rainer Wendt meinte, der Staat halte sich „geradezu künstlich dumm, wenn er weiter darauf verzichtet, dem Zusammenhang zwischen Kriminalität und Zuwanderungshintergrund nachzuspüren“ (DDP-Meldung 02.01.2009; Bayerisches Staatsministerium des Innern PM 10/09 v. 09.01.2009; Stoldt www.welt.de 07.01.2009).

Berlin

Zentrale SchülerInnendatei geplant

Die rot-rote Regierungskoalition im Land Berlin will eine zentrale SchülerInnendatei einrichten. Die Fraktion von SPD und Linken haben sich insofern auf einen gemeinsamen Gesetzentwurf geeinigt, wonach die SchülerInnen der Hauptstadt künftig durchnummeriert und 16 persönliche Informationen über sie automatisiert in einer zentralen Datenbank gespeichert werden sollen. Der

Gesetzesvorstoß wurde am 25.11.2008 erstmals im Datenschutzausschuss des Berliner Abgeordnetenhauses diskutiert. Gespeichert werden sollen Name, Geburtsdatum und -ort, Geschlecht, Anschrift, Ansprechmöglichkeit der Erziehungsberechtigten, Informationen zur besuchten Schule, die „nichtdeutsche Herkunftssprache", spezieller Förderbedarf oder „die Befreiung von der Zahlung eines Eigenanteils für Lernmittel". Verarbeitungs- und Zugriffsrechte sollen neben den zuständigen Schulen den bereichsspezifischen Schulämtern der Berliner Bezirke zustehen. Teilweise ist die Pflicht zur Pseudonymisierung von Daten vorgesehen. Auch die Senatsschulverwaltung soll automatisierten Zugriff grds. nur auf pseudonymisierte Daten erhalten; ein Zugriff auf Daten eines konkreten Schülers soll für sie ausgeschlossen sein. Die zuständige Senatsverwaltung darf gemäß dem Entwurf „auf Anfrage im Einzelfall" Strafverfolgungsbehörden, Polizei, Jugendämtern nebst Gerichtshilfe, der Bewährungshilfe und den Gesundheitsämtern „unverzüglich" mitteilen, welche Ausbildungsstätte eine SchülerIn besucht. Sie kann zudem Polizeibehörden „zur Abwehr einer konkreten Gefahr" allgemeine Personeninfos sowie Name, Anschrift und Telefonnummer der Erziehungsberechtigten übermitteln. Dafür soll eine gesonderte Stelle eingerichtet werden, die organisatorisch, personell und räumlich von anderen Organisationen des Schulressorts zu trennen ist. Die Daten wären ein Jahr nach Austritt aus der Schule zu löschen, wenn bis dahin die Schulpflicht nicht mehr besteht. Die Schülerdatei soll zum Beginn des neuen Schuljahrs im Spätsommer 2009 in Betrieb gehen können.

Die Koalition begründet ihren Plan v.a. damit, dass er zur besseren Organisation des Schuljahres beitragen könne. Damit wird Bezug genommen auf die Bedarfsplanung, die Gründung, Zusammenlegung, Umwandlung und Aufhebung von Ausbildungseinrichtungen, die Festsetzung der Aufnahmekapazitäten, die Vergabe von Schulplätzen sowie die Lehrkräftezuteilung. Künftig soll es nicht mehr möglich sein, dass Eltern ihre Schützlinge an mehreren Schulen anmelden. Ferner erhofft sich Rot-Rot einen Beitrag zur „Kontrolle und Durchsetzung der Schulpflicht". Bildungssenator Jürgen Zöllner (SPD) wünscht sich die Datei seit Langem, um eine bessere Übersicht zu erlangen, wie viele Lehrkräfte zum neuen Schuljahr einzustellen sind. Auch die Polizei forderte das Zentralverzeichnis, um straffällige oder schwänzende SchülerInnen schneller der entsprechenden Schule zuordnen zu können. In der Linksfraktion hatten einige Abgeordnete zunächst Bauchschmerzen, v.a. wegen der einfließenden Merkmale, weil damit ein Sozialprofil von Familien erstellt werden könne. Die Fraktionschefin der Linken, Carola Bluhm, erklärte sich aber mit dem nun vorliegenden Entwurf zufrieden, da ein „gläserner Schüler" nicht entstehe. Der stellv. Berliner Datenschutzbeauftragte Thomas Petri sieht den Entwurf mit gemischten Gefühlen. Einerseits regele er einen eingeschränkten Zugriff auf die Informationen. Andererseits berge eine zentrale Datei immer Risiken. Die Grünen kritisierten die „Datenschnüffelei in den Schulen", wenn die Daten wie geplant kommen. Aufgabe der Bildungsstätten sei es nicht, „als Hilfssheriff den Sicherheitsbehörden zu dienen". Die Oppositionspartei fordert die strikte Trennung von Personen- und Sozialdaten. Nur so könnten Stigmatisierung und Missbrauch verhindert werden. Die freien Schulen warnten vor einem „übertriebenen Datenhunger". Die Koalition kann dagegen mit der Unterstützung der CDU rechnen (Krempl, www.heise.de 26.11.2008).

Berlin

Kita-Fingerabdruckscanner für Eltern geplant

Der evangelische Kirchenkreis Berlin-Stadtmitte plant, für seine 17 Kindertagesstätten (Kitas) aus Sicherheitsgründen die Fingerabdrücke der Eltern zu speichern. Ziel eines Pilotprojektes im Zion-Kindergarten an der Griebenowstraße sei es zu verhindern, dass Unbefugte die Kinder mitnehmen. Die Erziehungsberechtigten sollen deshalb ihre Fingerabdrücke von einem Gerät auslesen lassen, wenn sie ihre Kinder in die Kita bringen und von dort abholen. Kirchenkreis-Geschäftsführerin Kathrin Janert betonte, die geplante dreimonatige Testphase werde nur mit Zustimmung der Eltern begonnen. Im Zion-Kindergarten mit mehreren Etagen und Ausgängen würden 85 Kinder betreut, da werde es schon mal unübersichtlich. Christiane Schimansky-Geier, Leiterin des Zion-Kindergartens, sieht in den gespeicherten Daten vor allem eine rechtliche Absicherung der Erzieherinnen und die Chance, im Notfall Klarheit über den Verbleib eines Kindes zu haben: „Erzieher können auch nicht überall ihre Augen haben." Hintergrund der Pläne ist ein Vorfall vor ca. 2 Jahren, bei dem Kinder ohne Aufsicht einen der Kindergärten verlassen hatten. Bei einem darauf folgenden Rechtsstreit zwischen Eltern und Kindergarten gab es v.a. Unstimmigkeiten über den genauen Betreuungszeitraum.

Auf einer Elternversammlung im Zion-Kindergarten gab es kontroverse Reaktionen, so Janert: „Einige Eltern waren strikt dagegen; andere haben ihren Fingerabdruck schon abgegeben. Während der Testphase könnten gelegentliche Abholer auch mit einer einfachen Vollmacht die Kinder abholen. Wenn ein Elternteil das Einscannen vergisst, tragen die Erzieher das Kind nachträglich aus dem Gerät aus. Janert ist sich der Lücken im System bewusst: „Am besten wäre es natürlich, über so eine Maschine die Türöffnung zu kontrollieren." Der Datenschutzbeauftragte der evangelischen Kirche Detlef Rückert bezweifelt die Rechtmäßigkeit des Projekts: „Im Datenschutzgesetz der Evangelischen Kirche Deutschland ist der Bezug von möglichst wenig personenbezogenen Daten festgeschrieben. Im Fall von Kindergärten bezweifele ich, dass es verhältnismäßig ist, die biometrischen Daten der Eltern zu speichern." Auch aus Sicht der Geschäftsführerin Janert müssen noch einige Datenschutzfragen geklärt werden, etwa, was mit den gewonnenen Daten gemacht werde. Nicht bewusst seien ihr die rechtlichen Hintergründe

gewesen und die Sensibilität von persönlichen Daten. Sie habe sich schlicht auf eine Erklärung der Firma verlassen, die das biometrische Zugangssystem verkauft hat. In den Niederlanden werden Fingerabdruckscanner schon seit geraumer Zeit als Zutrittskontrollen in Kitas genutzt und von den meisten Eltern auch akzeptiert (Marrenbach www.taz.de 24.11.2008; taz 25.11.2008, 7; www.heise.de 24.11.2008).

Hamburg

Verfassungsschutz sammelt Daten über Info-Stände

Seit dem 01.10.2008 leiten 5 von 7 Bezirken der Freien und Hansestadt Hamburg Angaben wie Name, Adresse, Telefonnummer, Email-Adresse und Zweck der Veranstaltung von allen Menschen an das Landesamt für Verfassungsschutz weiter, wenn diese für das Aufstellen eines Info-Standes eine Sondernutzungserlaubnis beantragen, egal, ob sie für eine Bürgerinitiative, einen Verein oder eine Kirche aktiv sind. Dies wurde als Antwort des Senats auf eine Anfrage der Bürgerschaftsabgeordneten der Links-Partei Christiane Schneider bekannt. In der Antwort vom November 2008 teilte der Senat mit, dass der Verfassungsschutz alle Bezirksämter ersucht hat, ihn auf die Email-Verteilliste über Info-Stände aufzunehmen. Dem seien 5 Bezirke nachgekommen, die in den ersten 6 Wochen Angaben zu 164 Ständen weitergegeben haben, wobei es sich v.a. um Parteien, aber auch um Hilfsorganisationen, Bürgerinitiativen, Kirchen und Einzelpersonen handelte. Der Verfassungsschutz begründete seinen Bedarf damit, bislang nur unvollständig über möglicherweise verfassungsfeindliche Veranstaltungen unterrichtet gewesen zu sein, so Behördenchef Heino Vahldiek: „Es gibt Leute, die sich als Bürgerinitiative organisieren und trotzdem extremistische Bestrebungen unterstützen.“ Es gehe um frühzeitige Informationen, falls Störungen durch Extremisten zu befürchten sind, etwa bei Ständen gegen Neonazis. Bei Unbedenklichkeit würden die Daten wieder vernichtet. Nach Angaben der Linken-Abgeordneten Schneider war unter den erfassten Ständen auch einer der Linkspartei in Bergedorf, bei dem zum Protest gegen einen Castor-Transport aufgerufen wurde: „Der Innensenator und der Präsident des Landesamtes für Verfassungsschutz verlassen den Boden der Rechtsstaatlichkeit, wenn sie die Grundrechte der Menschen in Hamburg aushebeln.“ Die mitregierenden Grünen zeigten sich irritiert. Deren Antje Möller meldete gegenüber CDU-Innensenator Christoph Ahlhaus „Gesprächsbedarf“ an: „Das Vorhaben des Verfassungsschutzes hätte im Parlamentarischen Kontrollausschuss behandelt werden müssen.“ Eben dort will die oppositionelle SPD das Behördenvorgehen erörtert wissen (SH-Z 14.11.2008, 5).

Nordrhein-Westfalen

900 Euro-Strafbefehl für 6 Mio. illegale Datensätze

Mit einer Geldstrafe von 900 Euro kommt der Adresshändler davon, der im Sommer 2008 illegal 6 Mio. Datensätze an den Verbraucherzentrale Bundesverband (vzbv) verkauft hat. Die Verbraucherschützer hatten den Deal verdeckt abgewickelt, um zu beweisen, wie einfach selbst sensible Konteninformationen auf dem Schwarzmarkt erworben werden können. Eine Strafanzeige des vzbv gegen den 22jährigen arbeitslosen ehemaligen Callcenter-Angestellten landete beim Amtsgericht Münster, das das Verfahren mit einem Strafbefehl beendete. Angesichts dieser Bagatellstrafe meinte der vzbv-Vorstand Gerd Billen: „Das Vorgehen belegt, dass gerade in der Verfolgung von Datenmissbrauch nachgelegt werden muss“. Die Ermittler seien offenbar nicht der Frage nachgegangen, woher die Daten letztlich stammten. Notwendig sei die Einrichtung von Schwerpunkt-Staatsanwaltschaften (Der Spiegel 4/2009, 19; SZ 19.01.2009, 5; www.heise.de 17.01.2009).

Nordrhein-Westfalen

WestLB verschickt versehentlich Kundendaten

Eine Mitarbeiterin der WestLB, der drittgrößten deutschen Landesbank, hat versehentlich eine Datei mit Daten von mehr als 800 GeschäftskundInnen per Email an einen völlig unbeteiligten Privatmann aus dem Kölner Umland verschickt, der die Daten in seiner elektronischen Post vorfand. Ein WestLB-Sprecher betonte, dass es sich nicht um Kontonummern, sondern um Firmenadressen und Ansprechpartner handelte: „Für Dritte ist diese Datei nicht zu verwerten.“ Die Mitarbeiterin wollte die Daten über das Internet an sich selbst mailen, um zu Hause daran zu arbeiten. Die Datei landete „auf Grund eines Buchstabendrehers in der Adresse“ in den falschen Händen (www.heise.de 18.12.2008; SZ 19.12.2008, 6).

Schleswig-Holstein

Zehntausende Karstadt-Kundendaten auf Autobahn verstreut

Zehntausende Kassenbelege aus Lastschriftverfahren haben am 18.12.2008 die Autobahn A7 zwischen Hamburg-Moorburg und Heimfeld kurzfristig lahmgelegt. Ein Kurierdienst von DHL hatte u.a. Kisten mit den unterschriebenen Kundenbelegen der Kieler Karstadt-Filialen während seiner Fahrt verloren. Ein nachfolgender Bus fuhr darüber; die Kisten wurden durch den Aufprall zerfetzt. Ein Polizeisprecher: „Die Papiere flatterten wie Schneeflocken über die Fahrbahn.“ Beamte sperrten die Autobahn für kurze Zeit und sammelten noch in der Nacht mit Taschenlampen die Ladung des Kuriers wieder ein. Teilweise mussten die Einsatzkräfte in den steilen, von Dornengestrüpp durchsetzten Hang neben der Autobahn klettern. Der Fahrer des Wagens hatte den Vorfall offensichtlich nicht bemerkt und war weitergefahren. „Es ging um den Datenschutz“,

sagte ein Polizeibeamter. Auf den Lastschriftbelegen befanden sich neben Informationen über die gekauften Artikel auch die Bankverbindungs- und Kreditkartendaten sowie die Unterschriften der KundInnen. Hauptkommissar Andreas Schöpflin: „Wir konnten einen Großteil der Belege sicherstellen.“ Der Rest sei vom Winde verweht. Schleswig-Holsteins Datenschutzbeauftragter Thilo Weichert: „Es handelt sich hier um hoch sensible Daten, mit denen durchaus Missbrauch getrieben werden kann, wenn sie in die falschen Hände gelangen.“ Da die Daten jedoch nicht gestohlen, sondern unbeabsichtigt verloren und rasch wieder eingesammelt wurden, bestehe in diesem Fall nur eine geringe Gefahr. Die Polizei will die Kosten für den Einsatz und die Sperrung der Autobahn von dem Transportunternehmen zurückverlangen (Kieler Nachrichten 20.12.2008, 15; www.welt.de 20.12.2008).

Internationale Datenschutznachrichten

Europa

Peter Hustinx bleibt Europäischer Datenschutzbeauftragter

Das Europaparlament und der Rat haben sich darauf verständigt, Peter Hustinx für eine zweite Periode als European Data Protection Supervisor (EDPS - Europäischer Datenschutzbeauftragter) zu benennen. Als Stellvertreter - ebenfalls für eine 5-Jahresperiode - wurde Giovanni Buttarelli benannt. Er ersetzt Joaquin Bayo Delgado, der sich nicht für eine zweite Amtszeit bewarb. Hustinx ist seit Januar 2004 EDPS und hat seine Dienststelle aufgebaut. Buttarelli war seit 1986 Mitglied der italienischen Gerichtsbarkeit und seit 1997 Generalsekretär der italienischen Datenschutzbehörde. 2002 bis 2003 war er Vorsitzender der Gemeinsamen Kontrollinstanz zum Schengenvertrag, der er 2000 bis 2001 als Vizepräsident angehörte. Er hatte Italien in einigen Komitees und Arbeitsgruppen im Bereich des Datenschutzes bei der Europäischen Union und beim Europarat vertreten (EDPS Press Release 23.12.2008).

Europa

Fluggastdatensammlung kommt vorläufig nicht

Die Bundesregierung will den Vorstoß der Europäischen Union (EU) zum Aufbau eines Systems zur Sammlung und Auswertung von Fluggastdaten mindestens bis zur Bundestagswahl im Herbst 2009 blockieren. Dies erklärte Brigitte Zypries (SPD) nach dem Ratstreffen der europäischen Justiz- und Innenminister am 27.11.2008 in Brüssel. Aus Deutschland werde es in der laufenden Legislaturperiode kein grünes Licht geben für die von der EU-Kommission geplante 13jährige Aufzeichnung von Passenger Name Records (PNR). Dies sei mit dem federführenden Bundesinnenminister Wolfgang Schäuble abgesprochen. Zypries meinte, das Vorhaben sei derzeit „in Deutschland nicht vermittelbar“. Sie persönlich halte es nicht für sinnvoll, z.B. jeden Bürger zu erfassen, der ein minderjähriges Kind am Flughafen abhole, oder die Vornamen von Ticketverkäufern im Reisebüro: „Mir kann kein Mensch sagen, dass das wirklich erforderlich ist für die Fahndung nach mutmaßlichen Terroristen.“ Die Bundesregierung will vor dieser weiteren Form der Vorratsdatenspeicherung das Urteil des Bundesverfassungsgerichts zur verdachtsunabhängigen Protokollierung von Verbindungs- und Standortdaten der Telekommunikation abwarten.

Kurz zuvor hatte die französische Innenministerin Michèle Alliot-Marie noch versichert, dass die Regierungsvertreter beim PNR-System vorangekommen seien. Auf die gravierenden Bedenken des EU-Parlaments habe man „Antworten gefunden“. Es gebe aber noch Auseinandersetzungen und offene Fragen. Der französische EU-Justizkommissar Jacques Barrot räumte ein, dass es noch unklar sei, ob und wann ein EU-PNR-System seine Arbeit aufnehme. Es könne beim Erkennen von Verbrechen nützlich sein, z.B. für die Bekämpfung des Menschen- und Drogenhandels. Zuvor war das Hauptargument für die Überwachungsmaßnahme die bessere Bekämpfung des Terrorismus. V.a. bei FDP-Politikern führte der französische Vorstoß zu Protesten, die Datensammlung auch auf innereuropäische Flüge auszuweiten, z.B. der innenpolitische Sprecher der Liberalen im EU-Parlament, Alexander Alvaro: „Die Verhältnismäßigkeit der Speicherung von ´zigfachen Datensätzen ist nach wie

vor nicht gegeben." Keiner habe bisher darlegen können, dass die Maßnahme effektiv sei. Unterstützend Nordrhein-Westfalens Innenminister Ingo Wolf (FDP): „Die uferlose Datensammelwut zum Zweck der Terrorismusbekämpfung muss gestoppt werden". Er lehnt nachdrücklich eine erweiterte PNR-Speicherung ab (Krempl, www.heise.de 28.11.2008 u. 27.11.2008; SZ 29./30.11.2008, 7)

Österreich

Athleten-Datenbank gegen Doping

Der Österreichische Skiverband (ÖSV) hat seinen AthletInnen ein Leben unter permanenter Beobachtung ver-ordnet, um Medikamentenmissbrauch einzudämmen. Unter der Leitung des Sportwissenschaftlers an der Universität Innsbruck Werner Nachbauer sammelt der ÖSV sämtliche Wettkampf- und Trainingsleistungen seiner SkifahrerInnen und dokumentiert, unter welchen Bedingungen, z.B. bei welcher Schneebeschaffenheit oder bei welchem Torabstand und welchem Gefälle bei AlpinsportlerInnen sie erzielt wurden. Erhoben werden der Umfang und die Intensität jedes Kraft- und Ausdauertrainings, die Ergebnisse von Gleichgewichts- und Psychotests, das Blutbild und Auswertungen von Spiroergometrie. 1,8 Mio. Datensätze sind inzwischen auf einem Server in Wien gespeichert - von Alpinen, LangläuferInnen und BiathlethInnen. Bis Mitte 2009 sollen auch Skispringer, Nordische Kombinierer und SnowborderInnen erfasst werden. Der ÖSV lässt sich die Datenbank 400.000 Euro kosten. Datenschutzbedenken verzögerten zunächst den Start. ÖSV-Präsident Peter Schröcksnadel, der nach den Doping-Razzien in den Quartieren der ÖSV-LangläuferInnen und BiathletInnen bei den Olympischen Spielen 2006 in der Kritik stand, meinte, mit der Datenbank könne man systematisch Doping ausschließen (Der Spiegel 2/2009, 103).

Frankreich

Magazin veröffentlicht Profil von ahnungslosem Webnutzer

Das französische Magazin „Le Tigre" verfasste auf der Basis von Eigeneintragungen in zahlreichen Online-Profilen wie z. B. bei Facebook, YouTube und Flickr von einem Nutzer ein detailliertes Portrait und veröffentlichte dies hübsch zusammengeschrieben in gedruckter Form. Hierzu hatten die Redakteure im Dezember 2008 den Mann per Zufall herausgepickt. In dem Portrait ist über Familie und Ex-Freundinnen sowie über seine Arbeit und Hobbys zu lesen; selbst seine Handynummer wird genannt. Der zuvor nicht eingeweihte Mann fühlt sich nun in seiner Privatsphäre verletzt. Das Portrait, in dem lediglich sein Nachname fehlte, habe ihm nächtelang den Schlag geraubt: „Ich habe sofort alle Angaben über mich im Internet gelöscht." Er protestierte schriftlich gegen den Text und bewirkte, dass die Zeitschrift seinen Wohnort und weitere Angaben in ihrer Internetausgabe verschleierte, um ihn nicht zusätzlich kenntlich zu machen. Die schon veröffentlichte Druckversion konnte natürlich nicht im Nachhinein geändert werden. Das Magazin wollte nach eigenen Angaben nur beweisen, dass es alles andere als harmlos ist, persönliche Informationen ins Internet zu stellen. Der Gründer des Magazins „Le Tigre" erläuterte: „Sein Privatleben im Internet auszubreiten ist gefährlich". Die Zeitschrift werde weitere „anonyme Portraits" von Internetnutzern veröffentlichen (www.spiegel.de 15.01.2009).

Großbritannien

Sozialdienst für StraftäterInnen nur in Leuchtwesten

Tausende britische StraftäterInnen, die Sozialdienst ableisten, müssen künftig Leuchtwesten tragen. Die Regierung kündigte am 01.12.2008 an, dass 10.000 orangene Westen mit der Aufschrift „Community Payback" (Wir müssen es bei der Gemeinde wieder gutmachen) verwendet werden. Menschenrechtsorganisationen kritisierten die Maßnahme scharf, so z.B. die Direktorin der Organisation Liberty, Shami Chakrabarti: „Wir hoffen, dass von dieser Mittelalter-Methode keiner Schaden davon trägt." Andere KritikerInnen äußerten Bedenken, dass die StraftäterInnen so Opfer von Angriffen werden könnten (SZ 02.12.2008, 8).

Großbritannien

Per Handy-Telemedizin dauernd unter Kontrolle

Mobiltelefone sollen in Zukunft Millionen chronisch Kranken helfen, ihren Gesundheitszustand besser zu überwachen. Forschende der Universität Oxford haben eine Software entwickelt, die PatientInnen in die Lage versetzt, Informationen z.B. zu Blutdruck oder den Blutzuckerspiegel auf einfache Weise über das Handy an einen Zentralrechner weiterzuleiten. Dort werden die Daten analysiert und das Ergebnis wird sofort automatisch zurückgemeldet; in dringenden Fällen ruft ein Krankenpfleger an. Der Ingenieur Lionel Tarassenko meint, dass sich die optimal überwachten PatientInnen nicht nur besser aufgehoben fühlten, sondern auch weitaus seltener die Notfallstation aufsuchen müssten. Das Gesundheitssystem spare so Millionen. Die Handy-Telemedizin wurde bisher von Tausenden PatientInnen erprobt und ist bereits in acht britischen Regionen im Einsatz. Die jährlichen Kosten dafür belaufen sich auf umgerechnet rund 300 Euro pro PatientIn (Der Spiegel 49/2008, 162).

Spanien

Mit Privatermittlern gegen private Urheberrechtsverstöße

Datenschützer haben die SGAE, das spanische Pendant zur deutschen GEMA (Gesellschaft für Musikalische Aufführungsrechte) wegen einer äußerst schwerwiegenden Verletzung der Intimsphäre zu einer Geldstrafe in Höhe von 60.101 Euro verurteilen lassen. Die SGAE hat die Aufgabe, Vergütungen für Urheberrechte, z.B. von Dichtern oder Komponisten, einzutreiben. Für diese Zwecke hatte die SGAE einen Privatermittler angeheuert, um eine Hochzeit ohne Wissen des Brautpaars zu bespitzeln. Dieser begab sich in das Restaurant „La Doma de San Juan Aznalfarache" bei Sevilla und zeichnete das Geschehen – Balz, Tanz und Völlerei – auf Video auf. Nach Auswertung dieser Aufnahmen wurde das Lokal von der SGAE wegen Nichtabführen von Aufführungsrechten zu einer Strafe von 43.179 Euro verurteilt. Ein andalusisches Handelsgericht gab der SGAE-Strafe statt, obwohl nur andere belastende Beweismittel, nicht aber das Video als Beweismittel zugelassen wurden. Der verfassungswidrigen Beweismittelbeschaffung nahm sich der Datenschutzverein Consumdato an und erhielt Recht. Eine SGAE-Sprecher zeigte sich aber wenig einsichtig: „Wir werden weiter Video benützen, um nachzuweisen, dass unsere Interessen verletzt werden." Consumdato hat unterdessen eine weitere Anzeige gegen die SGAE erstattet. Auch ein anderer Hochzeitsveranstalter ist von einem Detektiv ausgespäht und hernach mit einer Geldstrafe bedacht worden. Der Anwalt des Restaurants bei Sevilla meinte: „Wenn sie 40.000 Euro eintreiben und 60.000 Euro bezahlen müssen, bleibt ihnen ein Verlust von 20.000 Euro" (Caceres SZ 29.12.2008, 9).

Spanien

Videoüberwachung gegen Folter

Ein Gesetzentwurf, der am 12.12.2008 vom spanischen Kabinett beschlossen wurde, zielt darauf ab, den Umgang mit Terrorverdächtigen gemäß den Anregungen der UN-Menschenrechtskommission zu verbessern. Neben anderen Maßnahmen (Abschaffung von Isolationshaft für Minderjährige, Verkürzung der Zeit der Verweigerung anwaltlicher Beratung nach einer Verhaftung) ist die Anwendung des „Garzón-Protokolls" von Bedeutung. Dieses nach dem Untersuchungsrichter Baltasar Garzón benannte Festnahmeprotokoll, das seit zwei Jahren von einigen Richtern freiwillig angewandt worden ist, sieht die nahezu permanente Videoüberwachung von Gefangenen vor, die nach ihrer Festnahme in Isolationshaft kommen. Sie sollen in Zukunft von einem Vertrauensarzt und einem Amtsarzt untersucht werden und Familienbesuche erhalten können. Durch die Filmaufzeichnungen sollen einerseits Übergriffe von Beamten erschwert und andererseits die Sicherheitsbehörden gegen pauschale Foltervorwürfe geschützt werden. Eta-Terroristen waren in der Vergangenheit instruiert worden, Beamte in jedem Fall der Folter zu bezichtigen. Dies traf bisweilen auch zu. Anfang 2008 wurde die spanische Öffentlichkeit aufgeschreckt, als durch Fotos belegt wurde, dass Eta-Häftlinge verprügelt und unter Wasser gedrückt worden waren. Der Vorsitzende von Amnesty International Spanien, Esteban Beltrán, begrüßte die Videoüberwachung des Polizeigewahrsams. Beltrán forderte zugleich ein größeres Problembewusstsein im Umgang mit Festgenommenen, insbesondere von inhaftierten Einwanderern. Zuvor waren Beamte der katalanischen Regionalpolizei zu Haftstrafen verurteilt worden; sie waren per Video der Misshandlung eines Rumänen überführt worden (Caceres SZ 10.12.2008, 8).

Bulgarien

Oberstes Gericht stoppt Vorratsdatenspeicherung

Das oberste bulgarische Verwaltungsgericht hat mit einem Urteil vom 11.12.2008 die auch in Bulgarien Anfang 2008 umgesetzte Vorratsdatenspeicherung nach der EU-Richtlinie 2006/24/EC gestoppt. Danach ist die zur Umsetzung vom Innenministerium erlassene Verordnung Nr. 40 verfassungswidrig, weil damit die Sicherheitsbehörden nahezu unbegrenzten Zugriff auf persönliche Daten erlangen. Die Regierung wurde aufgefordert, verständliche und klar formulierte Begründungen für den Zugriff auf persönliche Daten und ihre Speicherung zu liefern. Das Urteil hob eine Entscheidung eines untergeordneten Gerichts auf. Geklagt hatte im März 2008 die Bürgerrechtsorganisation Access to Information Programme (API) mit dem Verweis auf Verstöße gegen die bulgarische Verfassung, die Europäische Menschenrechtskonvention und EU-Recht. Die Verordnung erlaubte den Sicherheitsbehörden in Art. 5 praktisch unbegrenzten Zugriff auf alle bei den Providern gespeicherte Daten ohne richterliche Genehmigung. Das Gericht rügte, dass keine klaren Begrenzungen des Zugriffs und keine Garantien für den nach Art. 32 der bulgarischen Verfassung geschützten Privatsphäre sowie „Ehre, Würde und Ansehen" einer Person vorgesehen sind. Außerdem werde Art. 8 der Europäischen Menschenrechtskonvention verletzt, wonach jede Person „das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz" hat. Ausnahmen darf es nur geben, „wenn der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer". Dies sei im beanstandeten Art. 5 der Verordnung nicht deutlich geregelt und begründet worden. Alexander

Kashumov, Rechtsvertreter der API in dem Verfahren, sieht in dem Urteil eine über das Land hinausgehende Bedeutung: „Die Entscheidung schützt nicht nur die Privatsphäre der Bulgaren und vor allem auch die Arbeit investigativ recherchierender Journalisten, die am meisten von Überwachung und Abhören bedroht sind. Sie kann auch für Bürger im übrigen Europa von Nutzen sein" (Telepolis, www.heise.de 23.12.2008).

USA

Zahl der Datenpannen 2008 massiv angestiegen

In den USA ist die Zahl der Datenpannen 2008 wieder enorm angestiegen. Gemäß einer Statistik des Identity Theft Ressource Centers in San Diego kam es im vergangenen Jahr in 656 Fällen zu dokumentierten Datenverlusten. Dies entspräche einer „dramatischen" Zunahme von 47% im Vergleich zu 2007, wo Unternehmen und Behörden 446 entsprechende Vorkommnisse meldeten. Insgesamt sollen 35 Mio. Datensätze 2008 abhanden gekommen sein. Die personenbezogenen Informationen seien nur in 8,5% durch Passwörter geschützt und in 2,4% der Pannen verschlüsselt gewesen. Die meisten Datenabflüsse finden dem Bericht zufolge in der Privatwirtschaft statt, auch wenn der Finanzsektor und Kreditkartenunternehmen sich stärker um Datensicherheit kümmern würden. Dazu gelernt habe auch der Regierungssektor unter Einschluss des Pentagons, der nur noch an dritter Stelle liege und seit 2006 fast 50% weniger Sicherheitsverletzungen melden müsse. Verantwortlich für die Datenschutzdebakel sei v.a. der Verlust von Laptops und anderen digitalen Speichermedien mit Verbraucherdaten gewesen. Es folgten der interne und externe Diebstahl sowie die unbeabsichtigte Veröffentlichung und Verbreitung persönlicher Informationen. Nicht zuletzt wären externe Dienstleister für Datenverluste verantworlich. Den rasanten, sich bereits im Sommer 208 abzeichnenden Anstieg erklären die ExpertInnen für Identitätsdiebstahl zum einen damit, dass tatsächlich immer mehr Kriminelle Daten von Firmen klauen. Andererseits sei auch der öffentliche Druck gestiegen, Datenpannen, wie von Gesetzen gefordert, zu melden. Das Identity Theft Resouce Center wertet Medienberichte und die Eigenangaben von betroffenen Organisationen aus, um seinen Jahresbericht zu erstellen. Den schwersten Unfall gab demnach die Investmentbank BNY Mellon Shareowner Services bekannt, der nach eigenen Angaben im Februar 12,5 Mio. Datensätze auf einmal abhanden gekommen sind. Sie wurden in einer Kiste mit unverschlüsselten Datenträgern aus einem nicht richtig verschlossenen Transportfahrzeug gestohlen (Krempl, www.heise.de 08.01.2009).

USA

Hacker spähen Kreditkartendaten aus

Bei dem Kreditkartendienstleister Heartland Payment Systems in Princeton/New Jersey sind im Jahr 2008 offenbar Kreditkartendaten in großem Umfang gestohlen worden. Heartland, das für 250.000 Firmen monatlich ca. 100 Millionen Kreditkartentransaktionen sowie Lohnzahlungen abwickelt, räumte ein, dass Computerforensiker im Rechnersystem der Firma ein Programm gefunden haben, das Kreditkartendaten ausspähen konnte. Wie viele KundInnen betroffen sind und welche, stand für die Firma zunächst nicht fest. US-Medien spekulieren, dass es sich um den größten Datendiebstahl überhaupt handeln könnte und dass viele Millionen KundInnen betroffen sein könnten. Die Kreditkartenunternehmen Visa und Mastercard hatten Heartland im Spätherbst 2008 auf eigenartige Transaktionen hingewiesen. Bei eigenen Untersuchungen kam aber zunächst nichts heraus. Erst nachdem die Firma externe Forensiker beauftragte, wurde die Späh-Software auf den Rechnern der Firma entdeckt. Heartland vermutet, dass es Opfer eines groß angelegten internationalen Online-Betrugs ist. Das US-Justizministerium und der Secret Service haben ihre Ermittlungen aufgenommen. Von dem Datenklau könnten auch deutsche Kartenbesitzer betroffen sein, wenn sie in der fraglichen Zeit in den USA waren und dort mit ihren Kreditkarten bezahlt haben (SZ 22.01.2009, 14, 22).

USA

Sony erhält Millionenstrafe für Datensammeln von Kindern

Der Musikkonzern Sony BMG muss wegen der Speicherung der Daten von Minderjährigen an die US-Verbraucherschutzbehörde FTC (Federal Trade Commission) eine Strafe von einer Million Dollar bezahlen, weil es im Internet die Daten tausender NutzerInnen unter 12 Jahren gesammelt und verbreitet hatte. Sony BMG, Tochter des US-Zweigs von Sony, hat Zugriff auf mehr als 1000 Internetseiten der SängerInnen, die das Unternehmen unter Vertrag hat. Viele der KünstlerInnen sind besonders bei Kindern und Jugendlichen beliebt. Sony soll auf knapp 200 Seiten bewusst Informationen von 30.000 Nutzenden unter 12 Jahren gesammelt haben (SZ 13./14.12.2008, 28).

USA

FISA-Berufungsgericht erklärt Abhören ohne Richterbeschluss für legal

Ein US-Berufungsgericht hat den inzwischen ausgelaufenen „Protect America Act" (PAA) für rechtmäßig erklärt. Das Überwachungsgesetz gestattete der National Security Agency (NSA) und anderen US-Sicherheitsbehörden das Abhören der internationalen Telekommunikation ohne Richtererlaubnis. Es handelte sich dabei um eine Übergangslösung zur Neufassung des Foreign Intelligence Surveillance Act (FISA), die von August

2007 bis Februar 2008 in Kraft war. Ein Telekommunikationsunternehmen hatte gegen die darin enthaltenen Auflagen zur Mithilfe beim Abhören von US-BürgerInnen geklagt, da es verfassungswidrige Verletzungen der KundInnenrechte befürchtete. Der weitgehend im Geheimen agierende FISA Court of Review (FISCR) befand in seinem Urteil vom August 2008, dass die Regierung ausreichend Schutzvorkehrungen gegen eine willkürliche Beschnüffelung von Nutzenden im Anti-Terrorkampf getroffen habe. Der Gesetzgeber habe „mehrere Ebenen handhabbarer Sicherungen" in den PAA eingebaut, meinte Bruce Selya, Chefrichter des Berufungsgerichts. Damit würden Individuen ausreichend vor ungerechtfertigtem Schaden bewahrt. Einzelne gestattete Eingriffe in die Grundrechte seien im Streben nach dem Schutz der inneren Sicherheit verhältnismäßig. Auf diesem Weg sollte die Regierung nicht unnötig „frustriert" werden durch die Gerichte. Die Argumente des Klägers tat die Kammer als „Lamento über das Risiko" ab, „dass Regierungsvertreter nicht nach Treu und Glauben handeln". Diese Gefahr bestehe aber auch, wenn eine Richtergenehmigung vorgeschrieben wäre.

Das Urteil bezieht sich auf ein nicht mehr aktuelles Gesetz. Inzwischen gilt eine weitere, aber nicht weniger umstrittene Ergänzung des Abhörgesetzes, die den Hilfssheriffs der US-Sicherheitsbehörden Straffreiheit zusichert. Bürgerrechtlerinnen haben gegen die entsprechende Immunitätsklausel Klage erhoben. Der Beschluss dreht sich auch nicht direkt um das Abhörprogramm der Bush-Regierung, das schon vor der gesetzlichen Regelung im PAA der NSA einen Freibrief für das Abhören von Telekommunikation ohne Richtererlaubnis ausstellte. Dennoch feierte die auslaufende republikanische Administration das Urteil als Bestätigung ihrer harten Linie bei der Terrorismusbekämpfung. Die Bürgerrechtsbewegung Electronic Frontier Foundation (EFF) äußerte sich besorgt, dass grundlegende Datenschutzbestimmungen der US-Verfassung „eliminiert" worden seien. Stattdessen habe das Gericht der Geheimniskrämerei der Bush-Regierung bei Überwachungsfragen die Absolution erteilt. Dass dabei auch Unverdächtige und Begleitpersonen ins Fangnetz der Geheimdienste geraten, habe bei den Richtern offensichtlich keine Rolle gespielt. Es werde eine Theorie des reinen Vertrauens in Regierungshandeln gepredigt, was für künftige Gerichtsentscheidungen im Streit um das Abhörprogramm wenig Gutes bedeuten könne (Krempl www.heise.de 16.01.2009).

USA

Obama bekommt spionagesicheres Handy

Der neue US-Präsident Barack Obama muss auf sein bisher genutztes Blackberry verzichten, darf aber weiterhin per SMS, Email oder Mobiltelefon kommunizieren. Hierfür erhält er ein „spionagesicheres", 3.350 Dollar (ca. 2.500 Euro) teures, speziell anfertigtes „Smartphone". Obama bezeichnete sich selbst als „Blackberry-Abhängigen". Vor seiner Vereidigung hatte er erklärt, die Sicherheitsdienste müssten ihm das geliebte Kommunikationsmittel schon „aus den Händen reißen". E-Mails und Anrufe von Freunden könnten ihm während seiner Amtszeit helfen, den Kontakt zur amerikanischen Alltags-Wirklichkeit nicht zu verlieren. Wegen Sicherheitsbedenken mussten US-Präsidenten während ihrer Amtszeit bisher weitestgehend auf Email-Kommunikation verzichten. Obamas Vorgänger George W. Bush soll gezwungen worden sein, den elektronischen Briefverkehr ganz einzustellen. Bill Clinton hatte als Präsident zumindest noch zwei Emails verschikken dürfen: eine um das Email-System zu testen, eine zweite, als er 1998 dem Astronauten John Glenn alles Gute für dessen Reise ins All wünschte. Die US-Geheimdienste befürchten, dass ausländische AgentInnen sich in das Internet-Postfach des Präsidenten hakken und vertrauliche Informationen in die falschen Hände gelangen können. Der Hersteller des Blackberry RIM (Research In Motion) ist ein kanadisches Unternehmen. Anspruchsvolle Geräte wie das Blackberry können durch das eingebaute Positionsbestimmungssystem GPS den Aufenthaltsort des Staatschefs preisgeben.

Dies soll bei der Sonderanfertigung mit dem Namen „Sectera Edge" nicht möglich sein. Sie wurde vom Rüstungskonzern General Dynamics entwickelt. Die Nationale Sicherheitsbehörde NSA hat es für militärische Zwecke frei gegeben und hält es für sicher. Das Gerät ist mit Programmen ausgestattet, die aber nicht als nur vertrauenswürdig gelten; Betriebssystem ist Windows Mobile, kommuniziert wird über den Internet Explorer und den Windows Manager. Allerdings ist das System speziell angepasst und „gehärtet" worden. Per Knopfdruck kann der Besitzer von offener auf verschlüsselte Kommunikation wechseln. Gespräche und Dokumente, die der höchsten Geheimhaltungsstufe unterliegen, sollen so nicht in unbefugte Hände geraten können. Einer weiteren Anforderung soll das Gerät genügen: Nach dem US-Recht muss sämtliche Korrespondenz des Präsidenten dokumentiert und archiviert werden; dies gilt auch für SMS (SZ 23.01.2009, 5; Hauck SZ 26.01.2009, 38).

Mexiko

Handynutzende werden in Nationaler Datenbank registriert

Nach dem Senat hat auch das Parlament in Mexiko einem Gesetz einstimmig zugestimmt, wonach binnen eines Jahres ein nationales Register aller Handynutzenden eingerichtet werden soll. Ziel ist die bessere Bekämpfung von organisiertem Verbrechen, Erpressung, Bedrohung und Entführung. Gemäß dem Gesetz müssen alle Handybesitzenden sich mit ihrem Gerät und der SIM-Karte durch den Provider registrieren lassen, ihre Adresse angeben, einen Lichtbildausweis vorlegen, Fingerabdrücke abliefern und eine Unterschrift leisten. Nicht fristgemäß registrierte Handys sollen ohne Recht auf neue Aktivierung gesperrt werden. Die

Provider müssen alle Verbindungsdaten ein Jahr vorhalten und auf Anfrage von Sicherheitsbehörden die persönlichen sowie die Verbindungsdaten binnen 72 Stunden übermitteln. Über 70% der MexikanerInnen, also mehr als 70 Mio. Menschen, telefonieren nach Regierungsangaben mit dem Handy. Hintergrund des Gesetzes ist eine Welle von Gewaltverbrechen in dem Land. Immer mächtiger werdende Drogenkartelle sind offensichtlich mit den Sicherheitsbehörden bis in die höchsten Etagen hinein verfilzt. Die bisherige von Präsident Felipe Calderón initiierte militärische Bekämpfung der Verbrecherorganisationen hatte bisher wenig Erfolg. Im Jahr 2008 wurden nach Zeitungsangaben mehr als 5.000 Menschen im Zusammenhang mit dem Drogenkrieg getötet. Da die Kriminellen Handys nutzen, um ihre Taten auszuführen oder der Verfolgung zu entgehen, hofft man mit der nationalen Datenbank der Handybenutzenden den Kriminellen ein wichtiges Instrument zu nehmen. Ob die Maßnahme nützt, ist fraglich: Kriminelle können Handys aus dem Ausland besorgen oder registrierte Geräte stehlen (www.heise.de 06.12.2008).

Japan

Initiative gegen Google Street View

In Japan hat sich die Initiative Kanshi Shakai o Kyohisuru (Kampagne gegen die Überwachungsgesellschaft) gebildet, die Straßenaufnahmen japanischer Städte durch Google-Kamerawagen verhindern will. Die Gruppe mit Rechtsanwälten und Professoren der Sophia University argumentiert, Google Street View verletze fundamentale Regeln der japanischen Kultur, wenn Ansichten von Häusern veröffentlicht werden. Die Erfolgschancen der Initiative werden jedoch skeptisch beurteilt, da ein japanisches Unternehmen mit Location View (https://www.locaview.com) bereits einen ähnlichen Service anbietet, der wie Street View auf Straßenaufnahmen basiert (Borchers www.heise.de 20.12.2008; zu Street View DANA 3/2008, 121).

Technik-Nachrichten

Schnurlos-Telefone leicht zu knacken

Forschende der Technischen Universität Darmstadt, u.a. der Informatiker Erik Tews, haben gemeinsam mit dem Chaos Computer Club (CCC) Sicherheitslücken bei Schnurlos-Telefonen entdeckt. Betroffen sind Geräte, die den meistgenutzten Standard für schnurlose Telefonie DECT verwenden. Ein Angreifer kann Daten über DECT illegal abhören, umleiten oder Anschlüsse für eigene Zwecke missbrauchen. Die erforderlichen Fachkenntnisse sowie Kosten und Zeitaufwand seien sehr gering. Die Kosten für die nötige Zusatz-Steckkarte für Laptops betragen gerade einmal 23 Euro. In das kleine Gerät werden einige zusätzliche Drähte gelötet. Mit spezieller Software kann man dann z. B. von einem Auto aus, das vor dem Haus geparkt wird, aktive Gespräche aufspüren und mitschneiden. Gar kein Problem besteht, wenn die Verschlüsselung zwischen Handapparat und Basisstation nicht aktiviert ist. Aber auch die Verschlüsselung stellte Tews und seine KollegInnen nicht vor große Probleme. Sie gaukelten dem Telefon einfach eine Basisstation vor, die meldete, sie beherrsche keine Verschlüsselung. Darauf stellte die Anlage auf Kommunikation im Klartext um; die Gespräche ließen sich danach aufzeichnen. Nachträgliche Sicherheits-Updates sind bei den meisten Geräten nicht möglich. Als sichere Alternative gelten v.a. Schnur-Telefone und reine WLAN-Telefone. Handys und öffentliche Mobilfunknetze sind von der präsentierten Sicherheitslücke nicht betroffen. Auf eine Anfrage von „Frontal 21“ bei 13 Herstellern hat nur einer geantwortet. Der Kommentar vom Bundesbeauftragten für Datenschutz Peter Schaar: „Jetzt ist es höchste Eisenbahn, technisch nachzurüsten und Verbraucher und Verbraucherinnen zu informieren.“ Die Verschlüsselung müsse verpflichtend gemacht werden. Das Bundeswirtschaftsministerium setzt dagegen auf freiwillige Selbstverpflichtung: „Spezielle mandative Sicherheitsstandards bezüglich Abhörsicherheit für Endgeräte existieren nicht und wurden bisher mit Rücksicht auf die Förderung des Wettbewerbs und ein möglichst breites Produktspektrum auch nicht unterstützt“ (Kieler Nachrichten 31.12.2008, 5; SZ 03./04.01.2009, 20; www.heise.de 20.01.2009).

Biochip aus Papier und Klebeband für 3 Cent

ChemikerInnen der Harvard University haben aus Papier und doppelseitigem Teppichklebeband einen Biochip gebastelt, mit dem sie die Diagnostik in armen Ländern verbessern wollen. Mit einem Laser frästen sie Löcher und Kanäle in das Klebeband. In das Papier wurden die entsprechenden Muster eingeätzt. Anschließend wurden die Papierlagen mit den präparierten Plastikstreifen verklebt, so dass ein dreidimensionaler Papierstapel entstand. Durch eine Probenöffnung auf der Oberseite fließen Blut-, Urin- und Wasserproben durch das verzweigte Kanalsystem im Innern des Stapels zu präparierten Testfeldern auf der Unterseite. Jedes Feld ist mit Reagenzien getränkt, die z.B. auf Zucker, Proteine oder Umweltgifte anspringen. Der gesuchte Inhaltsstoff in der Probe wird durch eine Farbreaktion angezeigt. Mit einem nur wenige Zentimeter messenden Prototypen sei es den Forschenden gelungen, gleichzeitig vier verschiedene Proben auf vier verschiedene Inhaltsstoffe hin zu untersuchen. Die reinen Materialkosten beziffert das Team auf 3 US-Cent. Hinzu kommen allerdings noch die Testreagenzien. Entsprechende Biochips aus Kunststoffen oder Glas kosten mitunter mehr als 100 US-Dollar (SZ 19.12.2008, 16).

Videobilder auf Ausweisdokumenten

Die Bundesdruckerei entwickelt Ausweisdokumente, auf denen nicht nur ein digitales Foto gespeichert wird, sondern eine ganze Bildsequenz, also ein kleiner Videofilm, bei dem der Inhaber des Dokumentes langsam seinen Kopf von rechts nach links dreht. Deren Sprecherin Iris Köpke kündigte an, dass die Technik in 3 bis 5 Jahren marktreif sein werde: „Beim Grenzverkehr geht es heute weniger um Fälschungen als um Identitätsdiebstahl.“ D.h. Ausweise werden gestohlen und von Menschen genutzt, die den eigentlichen InhaberInnen ähnlich sehen. Die Behörden wünschten sich schon seit langem, kurze Videosequenzen auf Identitätsdokumenten zu speichern. Die Anzeigen müssten aber robust, biegsam und sehr dünn sein. Die Bundesdruckerei arbeitet bei diesem Projekt mit dem südkoreanischen Konzern Samsung zusammen, dem Weltmarktführer für Anzeigenfolien aus organischen Leuchtdioden, kurz OLED. Eine besondere Variante soll für die Videoausweise zum Einsatz kommen. Diese Leuchtdioden sitzen auf einem Gitter, einer sog. Aktiv-Matrix, von der aus sie angesteuert werden. Die Energie dazu liefert das Magnetfeld des Lesegeräts. Die Ausweise müssen dafür näher als 10 Zentimeter sein. OLED-Anzeigen werden heute schon für kleine elektronische Geräte verwendet, z.B. für Handys (SZ 13./14.12.2008, 22).

Rechtsprechung

EGMR

Genproben aus DNA-Datenbank müssen vernichtet werden

Gemäß einem Urteil des Europäischen Gerichtshofs für Menschenrechte (EGMR) vom 04.12.2008 muss Großbritannien, genauer gesagt England, Wales und Nordirland, mehr als 1,6 Mio. Erbgut-Proben und Fingerabdrücke von Personen vernichten, die zuvor von allen strafrechtlichen Vorwürfen freigesprochen wurden. Die Straßburger Richter verabreichten eine besondere Schmach, dass sie den Engländern empfohlen, ausgerechnet dem Vorbild der Schotten zu folgen. Sie verurteilten die Praxis, Informationen unbegrenzt in Datenbanken aufzubewahren. Eine derart „pauschale und unterschiedslose“ Anwendung könne „in einer demokratischen Gesellschaft nicht als notwendig erachtet“ werden. Das Gericht gab damit zwei Briten recht, die die Vernichtung ihrer Datensätze verlangt hatten. Alle anderen 46 Mitgliedstaaten des Europarats bewahren DNA-Proben nur für eine bestimmte Anzahl von Jahren auf. In Schottland, das vom Gericht als Vorbild herangezogen wurde, werden die DNA-Profile sofort vernichtet, wenn ihre Besitzer von Vorwürfen freigesprochen werden. Ausnahmen gibt es nur für Fälle, in denen der Verdacht auf bestimmte sexuelle oder gewalttätige Vergehen besteht. Aber auch dann dürfen die Proben nur drei Jahre aufbewahrt werden. In den anderen Landesteilen des Vereinigten Königreichs werden von jeder verhafteten Person automatisch Proben genommen, die selbst dann nicht vernichtet werden, wenn keine Strafverfolgung eingeleitet wird. Dies gilt selbst für mindere Vergehen wie Betteln oder Trunkenheit.

Das britische Innenministerium verfügt über die größte Datenbank für Strafverfolgungszwecke der Welt mit 4,6 DNA-Proben und 7,5 Mio. Fingerabdrücken. Zum Vergleich: Das deutsche Bundeskriminalamt (BKA) hat in seiner Datenbank genetische Fingerabdrücke von 427.000 Personen. Die Datensätze dürfen nur dann länger aufbewahrt werden, wenn Verdachtsmomente weiter bestehen oder zusätzliche Ermittlungen notwendig sind. Das Straßburger Urteil bedeutet, dass das britische Unterhaus Gesetze ändern muss. Einen festen Zeitrahmen gibt es dafür nicht. Schon einmal, etwa 3 Jahre zuvor, forderte der Menschenrechtsgerichtshof die britische Regierung auf, Strafgefangenen das aktive Wahlrecht zuzugestehen - bisher ohne Erfolg. Schon 289 hat der EGMR Urteile gegen London gefällt. So eindeutig und harsch wie das jüngste Urteil ist aber bisher noch keines ausgefallen (S. and Marper v. The United Kingdom (Nos. 330562 and 30566/04; Koydl, SZ 06./07.12.2008, 8).

EuGH

Finnische Steuerdaten können journalistisch veröffentlicht werden

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 16.12.2008 entschieden, dass für die Verarbeitung von bei den Steuerbehörden erhältlichen Personendaten mit dem Ziel, einen Kurzmitteilungsdienst einzurichten, der es Nutzenden von Mobiltelefonen ermöglicht, sich die Steuerdaten fremder Personen zusenden zu lassen, als Ausnahme vom Datenschutz gelten kann, wenn dies allein zu journalistischer Zwecken dient. Anlass war ein Antrag des finnischen Datenschutzbeauftragten nach Beschwerden von Privatpersonen, den Gesellschaften Markkinapörssi und Satamedia zu untersagen, ihre Auskunftstätigkeit fortzuführen. Markkinapörssi erfasst seit Jahren bei den Steuerbehörden Personendaten, um diese jährlich aus-

zugsweise in den Regionalausgaben der Zeitschrift Verokörssi zu veröffentlichen. Die dort erfassten Informationen umfassen Namen und Vornamen von ca. 1,2 Mio. natürlichen Personen, deren Einkommen bestimmte Schwellenwerte überschreitet, sowie auf 100 Euro genau deren Einkommen aus Kapital und Erwerbstätigkeit und Angaben zur Besteuerung ihres Vermögens. Diese Informationen werden in alphabetischen Listen nach Gemeinde und Einkommenskategorie geordnet veröffentlicht. Markinapörssi und Satamedia, ein verbundenes Unternehmen, an das die Daten auf einer CD-ROM weitergegeben werden, schlossen eine Vereinbarung mit einem Mobilfunkunternehmen, das für Rechnung von Satamedia einen Kurzmitteilungsdienst einrichtete, der es Handy-Nutzenden ermöglicht, gegen Zahlung von etwa 2 Euro die in der Zeitschrift Verokörssi veröffentlichten Daten auf ihr Telefon senden zu lassen.

Der Korkein hallinto-oikeus, der als oberstes finnisches Verwaltungsgericht in letzter Instanz über den Antrag der Datenschutzbehörde auf Einstellung des Dienstes entscheiden muss, hat den EuGH um die richtige Auslegung der Europäischen Datenschutzrichtlinie 95/46/EG (EU-DSRL) ersucht. Das Verwaltungsgericht wollte v.a. wissen, unter welchen Voraussetzungen die in Rede stehenden Tätigkeiten als eine allein zu journalistischen Zwecken erfolgende Datenverarbeitung angesehen werden kann und demzufolge Ausnahmen bzw. Einschränkungen beim Datenschutz gemacht werden können. Der EuGH stellte die Anwendbarkeit der EU-DSRL fest, selbst wenn die verwendeten Behördendateien nur in Medien veröffentlichtes Material enthalten. Anderenfalls liefe die Richtlinie weitgehend leer. Es würde nämlich ausreichen, dass die Mitgliedstaaten Daten veröffentlichen ließen, um sie dem von der Richtlinie vorgesehenen Schutz zu entziehen. Um den Schutz der Privatsphäre und die Freiheit der Meinungsäußerungsfreiheit miteinander in Einklang zu bringen, sind die Mitgliedstaaten aufgerufen, Ausnahmen in Bezug auf den Datenschutz vorzusehen. Diese Ausnahmen dürfen allein zu journalistischen, künstlerischen oder literarischen Zwecken, die unter das Grundrecht der Freiheit der Meinungsäußerung fallen, gemacht werden, soweit sie sich als notwendig erweisen, um das Recht der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen.

In Anbetracht der Bedeutung der Freiheit der Meinungsäußerung in jeder demokratischen Gesellschaft müsste einerseits die damit zusammenhängenden Begriffe, zu denen der des Journalismus gehört, weit ausgelegt werden. Andererseits erfordere der Schutz der Privatsphäre, dass sich die Ausnahmen und Einschränkungen beim Datenschutz auf das absolut Notwendige beschränken. Der EuGH meint, dass Tätigkeiten wie die von Markkinapörssi und Satamedia, die Daten betreffen, die aus Dokumenten stammen, die nach nationalen Rechtsvorschriften öffentlich sind, als „journalistische Tätigkeiten" eingestuft werden können, wenn sie zum Zweck haben, Informationen, Meinungen oder Ideen, mit welchem Übertragungsmittel auch immer, in der Öffentlichkeit zu verbreiten. Journalistische Tätigkeiten seien nicht Medienunternehmen vorbehalten und könnte mit Gewinnerzielungsabsicht verbunden sein. Es ist nunmehr Sache des Korkein hallinto-oikeus, zu prüfen, ob die im Ausgangsverfahren in Rede stehenden Tätigkeiten ausschließlich zum Ziel haben, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten (www.juris.de 16.12.2008).

EuGH

Ausländerzentralregister diskriminiert Europäer

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 16.12.2008 entschieden, dass das deutsche Ausländerzentralregister (AZR) gegen das Europäische Gemeinschaftsrecht verstößt, weil es in Deutschland lebende BürgerInnen aus anderen EU-Staaten gegenüber Deutschen benachteiligt (Az. C-524/06). Geklagt hatte wegen des Verstoßes gegen das Diskriminierungsverbot ein Österreicher. Im AZR beim Bundesamt für Migration und Flüchtlinge in Nürnberg werden personenbezogene Daten aller AusländerInnen gesammelt, die sich länger als drei Monate in Deutschland aufhalten. Zugriff haben ca. 6.000 Behörden und andere Stellen, u.a. zur Durchführung ausländerrechtlicher Vorschriften, aber auch die Bundesagentur für Arbeit und Sozialhilfeträger. Gespeichert werden Name, Geburtsdaten, Herkunft, Wohnort, Aufenthaltstitel, aber auch Vorstrafen, Religionszugehörigkeit sowie personenbezogene Daten von Zoll, Landespolizeien und Geheimdiensten. Die Daten dienen u.a. auch statistischen Zwecken und werden von Polizeibehörden und Geheimdiensten genutzt. Der österreichische Selbständige, der in Deutschland lebt und arbeitet, hatte sich 1996 gegen die AZR-Speicherung gewendet. Das Verfahren ging bis zum Oberverwaltungsgericht Münster, das den Streit an den EuGH verwies. Dieser entschied, dass ein Staat grundsätzlich berechtigt ist, Informationen über AusländerInnen in seinem Staatsgebiet zu sammeln und Statistiken zu führen, mit denen Bevölkerungsbewegungen analysiert werden können. Allerdings müsse dem Erforderlichkeitsgebot im Sinne der Richtlinie zum Schutz personenbezogener Daten genügt werden. Anonymisierte Statistiken sind zwar erlaubt. Die personenbezogene Nutzung der Daten zur Kriminalitätsbekämpfung ist jedoch verboten, weil dies andere EU-BürgerInnen kriminalisierte. Der Kläger hatte bemängelt, dass es kein entsprechendes Zentralregister für deutsche Bürgerinnen gibt und er damit diskriminiert sei. Zumindest die Daten der 2,3 EU-AusländerInnen in Deutschland dürfen nach dem Richterspruch nicht mehr uneingeschränkt genutzt werden. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar begrüßte das Urteil. Das Bundesamt für Migration und Flüchtlinge müsse überprüfen, ob Daten von EU-Bürgern gespeichert sind und diese anonymisieren. Die Daten von EU-Bürgern, die nicht für aufenthaltsrechtliche Zwecke nötig sind, müssten „unverzüglich" gelöscht werden. Wenn das EU-Ausland kein Ausland mehr ist, müsse umso schärfer kontrolliert werden, dass die

Daten von EU-Bürgern für unzulässige Verwendungen gesperrt werden. Das Bundesinnenministerium betonte, man wolle erst die Urteilsbegründung prüfen (Borchers www.heise.de 17.12.2008; www.juris.de 16.12.2008; Gaserow FR 17.12.2008, 5, 11; Bolesch SZ 17.12.2008, 5).

BVerfG

Laptops im Gerichtssal verboten

Das Bundesverfassungsgericht (BVerfG) hat am 03.12.2008 in einem Beschluss auf den Eilantrag des Bremer Journalisten Eckhard Stengel entschieden, dass ein gerichtliches Verbot von tragbaren Computern (Laptops, Notebooks) im Gerichtssaal verfassungskonform ist (Az. 1 BvQ 47/08). Der Journalist wollte für seine Berichte über den „Holzklotz“-Prozess in Oldenburg einen Laptop in der Verhandlung verwenden. Die Kammer des ersten Senats des BVerfG bestätigte das vom Strafrichter ausgesprochene Verbot, obwohl sie die Begründung „nicht in jeder Hinsicht überzeugend“ fanden. Entscheidend war für das BVerfG, dass mittlerweile Laptops auch mit Mikrofonen und Kameras ausgestattet sein können. Deren Verwendung verstoße gegen das Gerichtsverfassungsgesetz und lasse sich kaum kontrollieren. Die Karlsruher RichterInnen räumten ein, dass ein erhebliches öffentliches Informationsinteresse an Berichten über den Prozess bestand und dass Laptops für JournalistInnen ein besonders effizientes Arbeitsmittel sind. Gleichwohl sei die mit dem Verbot verbundene Einschränkung der Pressearbeit gerechtfertigt. Den Medien werde weder der Zugang zur Verhandlung erschwert noch werde die Berichterstattung erheblich beeinträchtigt. Der Kläger hatte geltend gemacht, er habe in den Pausen kaum Zeit zum Schreiben und könne Zeitungen mit einem frühen Redaktionsschluss nicht beliefern. Journalisten-Vertreterinnen kritisierten den Beschluss (SZ 12.12.2008, 15; BVerfG PM v. 11.12.2008).

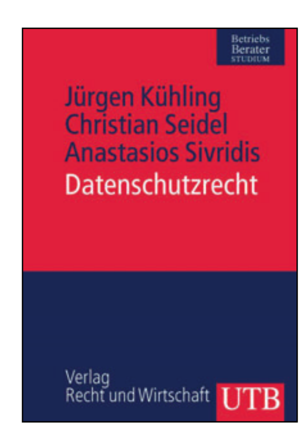
Niedersächsisches OVG

Rechtsgrundlage für Verbunddatei „Gewalttäter Sport“ unzureichend

Das Niedersächsische Oberverwaltungsgericht (OVG) hat mit Urteil vom 18.12.2008 die erstinstanzliche Entscheidung bestätigt, wonach es derzeit keine zureichende Rechtsgrundlage für die beim Bundeskriminalamt (BKA) geführte Verbunddatei „Gewalttäter Sport“ gibt (Az. 11 LC 229/08). Der Kläger hatte von der geklagten Polizeidirektion die Löschung personenbezogener Daten aus der beim BKA als Zentralstelle geführten Datei begehrt. Das Verwaltungsgericht (VG) Hannover gab dieser Klage statt mit der Begründung, dass es für die Führung der Datei „Gewalttäter Sport“ zurzeit keine ausreichende Rechtsgrundlage gibt, das eine in den §§ 11, 7 Abs. 6 BKA-Gesetz (BKAG) vorgeschriebene Rechtsverordnung noch nicht erlassen ist und die bestehende Errichtungsanordnung nach § 34 BKAG diese Rechtsverordnung nicht ersetzen kann (DANA 2/2008, 90 f.). Das Nds. OVG bestätigte die erstinstanzliche Entscheidung. Die Notwendigkeit der Datei „Gewalttäter Sport“ werde als solche nicht in Frage gestellt; es gehe im Berufungsverfahren ausschließlich um die formelle Frage der Rechtsgrundlage. Wegen der grundsätzlichen Bedeutung der Rechtssache hat der Senat die Revision an das Bundesverwaltungsgericht zugelassen.

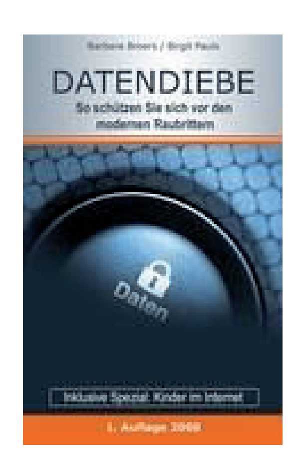
Zwischenzeitlich sind in der Datei „Gewalttäter Sport“ ca. 10.000 Personen gelistet. Dabei handelt es sich mehrheitlich um StraftäterInnen, aber auch um Fans, deren Personalien festgestellt worden sind, weil sie sich in der Nähe einer Schlägerei oder einer Demonstration aufgehalten haben. Eine gerichtliche Verurteilung ist für die Registrierung nicht nötig; es genügen polizeiliche Vermutungen. Die Folgen eines Eintrages können sein: Meldeauflagen, polizeiliche Hausbesuche, Passentzug oder Reiseverbot. Die Registrierten werden von den Behörden nicht über den Eintrag und den vorgesehenen Löschtermin informiert. Daher ist es schon vorgekommen, dass Registrierte ihren Urlaub auf dem Abflug-Flughafen beenden mussten, weil im Ausland zufällig ein Fußballspiel stattfand. Fragwürdig ist auch die Weitergabe der Daten an europäische Länder, wo es keine einheitlichen Datenschutzregelungen gibt. Registrierte wurden im Ausland schon in Gewahrsam genommen und drangsaliert. Seit Jahren kritisiert der Bundesbeauftragte für Datenschutz (BfDI) Peter Schaar die Strukturen beim BKA und dem übergeordneten Bundesministerium des Innern (BMI). Das BMI verteidigte die Datei und verwies auf anderslautende Gerichtsurteile: „Wir wollen mit der Datei die schwierige Arbeit der Polizei schützen“. Wilko Zicht, Sprecher des Bündnisses aktiver Fußballfans (Baff), will BKA und BMI unter Druck setzen. Möglich seien Schadensersatz- und Löschungsforderungen. Zahlreiche Fans haben mit dem Hinweis auf das erstinstanzliche Urteil des VG Hannover schon Anträge gestellt (www.juris.de 17.12.2008; PI Nds. OVG 17.12.2008; Blaschke, www.taz.de 09.01.2008; vgl. DANA 3/2005, 17 f.; Hülsmann, DFB-Fan-Kongress, DANA 3/2007, 122; Weichert, Die Fußball-WM als Überwachungs-Großprojekt, DANA 1/2005, 7).

Buchbesprechung



Kühling, Jürgen/Seidel, Christian/ Sivridis, Anastasois,
Datenschutzrecht, UTB, Verlag Recht und Wirtschaft Frankfurt a.M., 2008, 295 S.

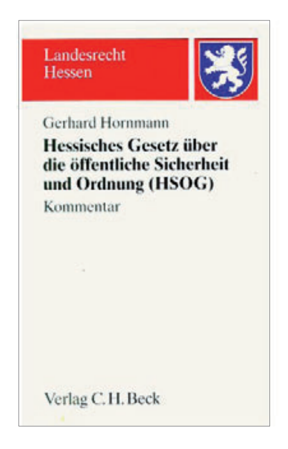
(tw) Man kann wohl noch nicht behaupten, dass das Datenschutzrecht im Lehrbetrieb der rechtswissenschaftlichen Fakultäten der Universitäten angekommen wäre. Aber jetzt gibt es wenigstens ein universitäres Lehrbuch. Von den drei Autoren scheint selbst Eingeweihten nur der Hauptautor Jürgen Kühling bekannt: Prof. Jürgen Kühling, früherer Verfassungsrichter, hat bei der Vorstellung des Grundrechte-Reports 2007 angesichts der Vorratsdatenspeicherung u.a. das Grundrecht auf Fernmeldegeheimnis als „Totalverlust" beklagt. Doch im Autorenportrait am Ende des Lehrbuchs lächelt einem ein 37 Jahre alter, erst seit 2007 in Regensburg tätiger Universitätsprofessor Dr. ius., LL.M. (Brüssel) entgegen. Vielleicht ein Verwandter mit gleichem Namen?! Jedenfalls das Buch ist vorzeigbar. Nicht als großer Wurf, dafür aber akribisch und qualifiziert wird hier das Datenschutzrecht - ausgerichtet für Jura-StudentInnen - präsentiert. Geradezu klassisch werden erst die internationale, dann die unionsrechtlichen und verfassungsrechtlichen und schließlich ausführlich die einfachgesetzlichen Grundlagen des Datenschutzes referiert, wobei systematisch die wichtigsten Regelungen erläutert werden, garniert mit etwas Rechtsprechung und Literatur. Orientierungsrahmen sind die Normen; Bezug genommen wird auf die Standardliteratur. D.h. eine wissenschaftliche Auseinandersetzung findet nur am Rande statt, Technik wird als Gegenstand des Rechts präsentiert; die in der Praxis hohe Bedeutung der Datenschutzbehörden drängt sich nicht gerade auf. In eher nüchterner Sprache werden alle wichtigen Aspekte dargestellt, wobei im nationalen Recht das Bundesdatenschutzgesetz im Zentrum steht, aber auch ausführlich das Telemedien- und das Telekommunikationsrecht referiert werden. Sonstiges bereichsspezifisches Datenschutzrecht sowie Randbereiche wie z.B. das Medizindatenschutzrecht mit dem Patientengeheimnis kommen nicht vor. Dies ist wohl einem akademischen Lehrbuch geschuldet. Anschaulich sind 14 Fallbeispiele, die zumeist am Kapitelende schulmäßig juristisch mit Lösungsskizzen durchgeprüft werden. Dort, wo die Autoren unterschiedliche Meinungen referieren, nehmen sie - zurückhaltend, aber durchgehend - grundrechtsfreundliche Positionen ein. Erfreulich ist auch, dass zumindest ein kleines Kapitel der Modernisierung des Datenschutzrechts gewidmet ist. Für Studierende kann dieses Buch also ohne Einschränkungen empfohlen werden, zumal die Inhalte gut strukturiert und über die nötigen Verzeichnisse (Inhalt, Abkürzung, Literatur, Stichworte) gut erschlossen sind. Für betriebliche, behördliche oder anwaltliche Praktiker ist das Buch nur als erster Einstieg geeignet; die Praxis stellt dann doch Fragen, die allein mit diesem Grundlagenwerk nicht beantwortet werden (können).



Broers, Barbara/Pauls, Birgit, Datendiebe - So schützen Sie sich vor den modernen Raubrittern, Books on Demand Norderstedt, 1. Aufl. 2008, ISBN 978383706224, 153 S., 12,80 Euro

(tw) Das kleine Büchlein von Broers/ Pauls ist für die NormalverbraucherIn, nicht die DatenschutzpraktikerIn oder die WissenschaftlerIn geschrieben. Für die Letzteren gibt es ja inzwischen sehr viel Literatur, so aber nicht für Menschen, denen auf einfache aber eindringliche Weise Ziel und Nutzen des Datenschutzes vermittelt wird. Und das gelingt den Autorinnen im leichten Erzählstil. Cold Calls, Gewinnspiele im Internet, Phising, Viren, Würmer und Trojaner, übers Internet geworbene Geldwäscher, Spam, Handyortung - das sind die Stichworte zu den kurzen Geschichten, über die eine eindrückliche Sensibilisierung zur Datensparsamkeit, zur persönlichen und zur technischen Vorsicht und zu den Risiken im Netz - und nicht nur dort - erfolgt. Es werden Tipps gegeben zu kostenlosen Email-Accounts, zur effektiven Löschung von Rechnerfestplatten und zum Verhalten bei Foren und Chats, in sozialen Netzwerken und zur Heranführung von Kindern an den Datenschutz und zur Vermittlung von Medienkompetenz im Internet. Der Anhang enthält vorformulierte Standardtext zur Inanspruchnahme von Betroffenenrechten, die zuvor er-

läutert wurden, einige Gesetzesauszüge und einige brauchbare Adressen. Das alles wird in eingängiger Form und in einer leicht verständlichen Sprache präsentiert. Also das richtige Geschenk für Jemanden, der meint, er habe nichts zu verbergen, oder der allzu sorglos die neuen Medien nutzt. Es gibt natürlich nur erste Tipps, wer Genaueres wissen möchte, der muss sich dann wo anders informieren. Dass dies auch im Internet möglich ist, ist bei den genannten Adressen nicht eindeutig zu erkennen. Im Anhang finden sich auch drei Musterschreiben für Werbe- und Kontoabbuchungswiderspruch sowie Auskunft. Die Autorinnen wollen in Kürze einen „Band 2 der Datendiebe" veröffentlichen. Das Büchlein ist nett, unterhaltsam und kann im Einzelfall nützlich sein. Doch ist es relativ beliebig aufgebaut und daher wirklich nur zur allerersten Sensibilisierung geeignet. Wer etwas genauer wissen will, wird oft ohne Hilfen bleiben.



Gerhard Hornmann,
Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG), Verlag C.H. Beck, 2. Auflage, 2008 XXXXIV, 1110 Seiten, kartoniert € 79,00, ISBN: 978-3-406-58168-7

(hs) Heute gibt es keine staatlichen Stellen und Private mehr, die Angaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten) nicht mittels immer preiswerterer und leistungsfähigerer EDV verarbeitet. Mit Hilfe der EDV sind heute personenbezogene Daten technisch gesehen unbegrenzt speicherbar, in Sekundenschnelle abruf- und übertragbar und sie können mit anderen Datensammlungen in vielen Bereichen zu einem weitgehend vollständigen Persönlichkeitsbild zusammengeführt werden, ohne dass die betroffene Person dessen Richtigkeit und Verwendung zureichend kontrollieren kann, mit anderen Worten: Wir sind gläsern (Seite 229/230). Diese Aussage des Autors sagt fast alles über den Umgang mit personenbezogenen Daten – auch im Bereich des Polizei- und Ordnungsrechts. Insoweit soll der vorliegende Kommentar hier auch nur aus der Sicht des "Datenschutzes" besprochen werden.

Bei dem vorliegenden Werk handelt es sich um einen Kommentar zu einem bereichsspezifischem Gesetz, dem Hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG). Ohne personenbezogene Daten ist aber Polizeiarbeit nicht möglich und daher enthält nicht nur das HSOG eine Vielzahl von Normen zum Umgang mit personenbezogenen Daten im weiten Bereich der Gefahrenabwehr, sondern befasst sich auch der vorliegende Kommentar – auf dem Stand 1. Mai 2008 – sehr umfangreich und mit vielfachen Ausführungen mit dem Thema "Datenschutz". Insoweit verweist der Verfasser zu Recht darauf, dass eine typische Begleiterscheinung der EDV das Ansteigen der Neigung zur Datensammlung sei, je leichter, sparender und preiswerter Daten verarbeitet werden können, aber auch auf die Gefahr, sich bei zunehmender Arbeit mit der EDV auf die gespeicherten Angaben zu verlassen (Seite 232). Die Vorstellungen aus Orwells "1984" bekommen Konturen – wenn auch aus anderer Blickrichtung, die man sich 1984 mit der damaligen EDV, den komplizierten Datenaustauschmöglichkeiten und den geringen Speicherkapazitäten nicht vorstellen konnte.

Wie der Kommentator zu Recht erkennt, ist die Schutzgewährung im privaten Bereich lückenhaft (Seite 232), während gerade im Bereich der öffentlichen Sicherheit eine regelrechte Regelungswut herrscht, welche das Recht auf informationelle Selbstbestimmung zunehmend aushöhlt. Der Autor fordert daher – gestützt auf den ehemaligen Richter des BVerfG Grimm – dringend (wieder) eine Balance zwischen Bürgerfreiheiten und Sicherheitsbedürfnis des Staates zu finden, denn der allwissende Staat werde schnell zum allmächtigen Staat, und Freiheit gebe es dagegen nur im begrenzten Staat (Seite 234).

Unter dem Gesichtspunkt, dass der staatliche Eingriff in den absolut geschützten Achtungsanspruch des Einzelnen auf Wahrung seiner Würde (Art. 1 Abs. 1 GG) ungeachtet des Gewichts der betroffenen Verfassungsgüter stets verboten ist, befasst sich Gerhard Hornmann bei seiner Kommentierung der einzelnen Normen sehr intensiv und z.T. auch äußerst kritisch mit den durch die Normen gebotenen Eingriffsintensitäten, sei dies bei der Videoüberwachung oder – um eines der aktuellsten Schlagwörter zu nennen – bei der Vorratsdatenspeicherung (vgl. § 15 a Rdnrn. 55 - 77) oder dem IMSI-Catcher zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunksendegerätes. Sagte doch schon der ehemalige NSA-Agent Edward Lyel, in dem Film "Der Staatsfeind Nr. 1" zu dem seiner Identität beraubten Rechtsanwalt Robert C. Dean: "Je mehr Technologie wir verwenden, desto leichter ist es für die, uns zu überwachen. Es ist Orwells Welt da draußen.".

Dabei behält der Autor auch andere bereichsspezifische Regelungen zum Umgang mit personenbezogenen Daten im Auge, wie die StPO, die Verfassungsschutzgesetze, aber auch so unscheinbare, aber eingriffsintensive Gesetze wie das Seeaufgabengesetz (vgl. auch DANA 4/2008, S. 141 f.).

Die Kommentierung der datenschutzrechtlichen Normen ist genauso umfangreich wie die der übrigen Normen des Hessischen Polizeigesetzt. Dabei weist der Autor gezielt auf Schwächen des Gesetzes und mögliche Grenzen hin, bei denen verfassungsrechtliche Bedenken begründet sind, wie z.B. bei der offenen Videoüberwachung (§ 14 Rdnrn. 34 ff.), welche auch in Deutschland zunehmend Raum gewinnt. Dies obwohl im "Mutterland" der Videoüberwachung zunehmend kritische Stimmen auch aus dem Polizeibereich die Effektivität

bestreiten, ja der Einsatz sich für Scotland Yard als völliges Fiasko erwiesen hat (siehe DANA 2/2008, S. 83 f.). Auch wenn Hornmann auf diese Auslandserfahrungen nicht eingeht, so sind seine Ausführungen doch sehr lesenswert.

Andererseits sieht und erläutert der Autor auch, dass die Rechte der Betroffenen, um deren Daten es geht, eher rudimentär und lückenhaft geregelt sind (§ 13 Rdnr. 38).

Insgesamt sind die Aufführungen in dem vorliegenden Kommentar zum Umgang mit personenbezogenen Daten nach dem Hessischen Gesetz über die öffentliche Sicherheit und Ordnung sehr fundiert und zeigen, dass der Verfasser sich mit der Materie sehr gut auskennt. Insoweit ist es im Hinblick auf die Komplexität der Materie verzeihlich, wenn bezüglich der Einwilligung des Betroffenen auf § 183 BGB statt auf die spezifische Einwilligungsnorm des § 7 Abs. 2 HDSG, welche eine Aufklärung des Betroffenen voraussetzt, abstellt (§ 13 Rdnr. 74).

Neben einem Inhalts- und Literaturverzeichnis runden der Abdruck der ergänzenden Rechtsverordnungen und Verwaltungsvorschriften den Kommentar ab, wobei ein umfangreiches Stichwortverzeichnis das Erschließen des Werkes im Einzelfall statt über die Gesetzesparagraphen wesentlich erleichtert.

Insgesamt handelt es sich bei dem Werk um einen Kommentar, der neben der juristischen Ausbildung (Studenten und Referendare) gerade an die Praktiker, die Polizei und die Politik und damit auch an den Gesetzgeber gerichtet ist und – insbesondere letztem dringend zur Qulitätssicherung seiner Gesetze – empfohlen werden muss.



Florian Meininghaus,
Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren,
356 Seiten, Verlag Dr. Kovac, Hamburg 2007, 88,00 €, ISBN-10 38300-3158-0, ISBN-13 978-300-3158-1

(hs) Bei dem vorliegenden Werk handelt es sich um eine Dissertation, welche von der Juristischen Fakultät der Universität Passau angenommen wurde; sie geht aber über den Wert einer Dissertation weit hinaus. Denn der Verfasser untersucht bei seinen Ausführungen den Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 27.11.2006, welcher mit Gesetz vom 21.12.2007 (BGBl I 2007, 3198) Realität wurde, bereits mit. Insoweit ist das Werk auf einem aktuellen Stand bei den Fragen, die im Zusammenhang mit der E-Mail-Kommunikation stehen. Dabei beschränkt sich der Verfasser bewusst auf den Bereich der E-Mail. Gibt es doch bereits hier genug Rechtsfragen.

Auch wenn es sich um eine strafrechtliche Dissertation handelt, so ist sie nicht nur für Strafrechtler von Interesse, sondern betrifft jeden, der sich der E-Mail-Kommunikation bedient, sei dies als Anwender oder Anbieter entsprechender Leistungen. Dabei sind die Ausführungen verständlich aufgebaut und nehmen auch auf die Rücksicht, die nicht über umfassendes technische Verständnis verfügen, denn der Autor stellt seinen rechtlichen Überlegungen zunächst für den Leser die technischen Grundlagen, die Bedeutung des Zugriffs auf E-Mails und die Frage der tatsächlichen Zugriffsmöglichkeiten incl. der Kryptographieproblematik verständlich voran, so dass eine ordentliche Ausgangsbasis für die weiteren Erwägungen gelegt ist.

Der Verfasser legt in seinen weiteren Ausführungen und Überlegungen nachvollziehbar dar, dass eine E-Mail während des gesamten Übertragungsvorganges durch das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG geschützt ist, während außerhalb des Übertragungsvorganges stehende Mails durch das Recht auf informationelle Selbstbestimmung geschützt werden, wobei das Fernmeldegeheimnis erst bei aus der Mailbox abgerufenen Mails endet, auch wenn sie weiterhin auf der Mailbox gespeichert sind. Dies entspricht auch der Judikatur des Bundesverfassungsgerichts. Dabei weist der Autor zurecht auf die Probleme hin, die durch die eingeschränkte Definition des Fernmeldegeheimnisses im Telekommunikationsgesetz entstehen.

Auch wenn der Verfasser noch nicht die Entscheidung des BVerfG zur Onlinedurchsuchung und damit das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme kannte, erkennt der doch richtig, dass wegen der Unabhängigkeit von herkömmlichen räumlichen Barrieren der Zugriff über Datenleitungen auf einen Rechner nicht am Grundrecht des Art. 13 Abs. 1 GG in Bezug auf den Standort des Gerätes zu messen ist, sondern stützt sich insoweit auf das Recht auf informationelle Selbstbestimmung. Denn der "gespeicherten Privatheit" trage das Grundrecht auf informationelle Selbstbestimmung ausreichend Rechnung.

Die einzelnen Ausführungen und Überlegungen zu den Normen der Strafprozessordung und insbesondere des Telekommunikationsgesetzes sind in sich nachvollziehbar, auch wenn an der ein- oder anderen Stelle noch weiterer Diskussionsbedarf bestehen könnte.

Neben einer gut untergliederten Inhaltsübersicht befindet sich am Ende des Werkes noch ein Literaturverzeichnis. Was leider fehlt, ist ein Stichwortverzeichnis,

was aber insoweit verzeihlich sein mag, als die Inhaltsübersicht ebenfalls eine Erschließung einzelner Fragen ermöglicht.
Insgesamt handelt es sich bei der vorliegenden Dissertation um einen wichtigen Betrag in der Strafrechtspflege, welcher alle angeht, die mit dem Umgang von E-Mails befasst sind.



Schaffland, Hans J / Wiltfang, Noeme Bundesdatenschutzgesetz (BDSG) – Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften,

Loseblattausgabe, Stand: Lieferung 1/08, April 2008, Kunststoff Ordner, 2244 S. - 21 x 14,8 cm, Erich Schmidt Verlag, 98,00 Eur, ISBN 978-3-503-01518-4

(hs) Der Kommentar von „Schaffland/ Wiltfang“ zum Bundesdatenschutzgesetz will einen erleichterten Einstieg in die Wirren des Datenschutzrechts liefern. Deshalb bietet er dem Nutzer neben Inhaltsübersicht und ausführlichem Stichwortverzeichnis zunächst eine nicht unerhebliche Zahl von Gesetzen und Regelungen mit datenschutzrechtlichem Bezug, die es außerhalb des Bundesdatenschutzgesetzes gibt; neben den Landesdatenschutzgesetzen u.a. das Übereinkommen des Europarates zum Schutz der Menschen bei der automatisierten Verarbeitung personenbezogener Daten und die EG-Datenschutzrichtlinie incl. der Erwägungsgründe. Auch werden in Auszügen viele bundesgesetzliche Normen mit datenschutzrechtlichem Bezug abgedruckt, wie das Melderechtsrahmengesetz, das Geldwäschegesetz, das Telekommunikationsgesetz, die Sozialgesetzbücher, Pass- und Personalausweisgesetz und vieles mehr.

Auch wenn nach der Verlagsankündigung die Auszüge aus den wichtigsten vom BDSG tangierten Gesetzen einen Zugriff auf andere Gesetzesveröffentlichungen entbehrlich machen sollen, wäre der Nutzer schlecht beraten, sich immer hierauf zu verlassen. So ist z. B. die “Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Telekommunikationsdienstunternehmen-Datenschutzverordnung)” vom 12.07.1996 (Nr. 2067 des Werkes) nur bis zum 19.12.2000 gültig gewesen und durch die Novellierung des Telekommunikationsgesetz (TKG) außer Kraft getreten. Demgegenüber hat das Telekommunikationsgesetz vom 22.06.2004 (Nr. 2050 des Werkes) durch das Gesetz zur Änderung telekommunikationsrechtlicher Vorschriften (TKomÄndG) vom 18.02.2007 (BGBl I 2007, 106), aber auch durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (TKÜNReglG) vom 21.12.2007 (BGBl I 2007, 3198) gerade bei den datenschutzrechtlich relevanten Normen wesentliche Änderungen erfahren. Auch sind das Passgesetz, das SGB X, das HGB und andere Gesetze nicht auf dem Stand von Anfang 2008.

Dies schmälert die Bemühungen der Autoren, gerade dem betrieblichen oder behördlichen Datenschutzbeauftragten wertvolle Hinweise für die tägliche Arbeit zu geben, und verwässert die durchaus nutzbare Kommentierung.

Auch sind die am Ende des Werkes abgedruckten Hinweise der Aufsichtsbehörde für die private Wirtschaft seit der Novellierung des Bundesdatenschutzgesetzes und der Umsetzung der EG-Datenschutzrichtlinie in vielen Fällen für den Nutzer nicht sehr hilfreich, weil sie sich zu nicht mehr geltendem und damit überholtem Recht äußern. Insoweit hat der größte Teil der Anwendungshinweise nur noch historischen, aber keinen praktischen Wert mehr.

Insgesamt ist der Ansatz des Werkes sehr positiv und es wäre sehr zu wünschen, dass es den Herausgebern gelingt, mit den nächsten Nachlieferungen das Werk auf einen Stand zu bringen, der aktuell und damit für den Nutzer besser verwertbar ist – wofür die Grundlagen eigentlich gelegt sind. Bis zu diesem Zeitpunkt hilft auch eine klare Gliederung und eine Vielzahl praktischer Beispiele nur bedingt bei der Lösung tagesaktueller Probleme und ist daher aktuell nur unter Vorbehalt zu empfehlen.



Stellt der Datenschutz Weichen für den Standort Deutschland ? – Welche Regeln dem Verbraucher tatsächlich nützen – und wie viel Regulierung die deutsche Wirtschaft im internationalen Wettbewerb noch verträgt

3. SCHUFA Datenschutzkolloquium am 12. März 2008 in Berlin, 117 Seiten, Herausgeber SCHUFA Holding AG, Wiesbaden, ISBN 978-3-00-025090-3 oder auch auf 2 DVDs

(hs) Man stelle sich vor, man möchte einen Kredit für eine Hausfinanzierung bei einer Bank erhalten und gleich, bei welcher Bank man nachfragt, es gibt

keinen Kredit. Und dies, obwohl man der festen Überzeugung ist, auf Grund seiner finanziellen Verhältnisse, seines sicheren Berufes und aller sonstigen Umstände eigentlich kreditwürdig sein zu müssen. Dies wäre vielleicht auch so, hätte man nicht aus beruflichen Gründen mehrfach umziehen müssen und für die ganze Familie vier Handyverträge auf eigenen Namen abgeschlossen. Alles an sich nicht schlimm, aber es konnte zumindest bisher zu einer wesentlichen Verschlechterung des so genannten Score-Wertes führen, an dem sich die Banken bei der Vergabe von Krediten orientieren. Kein Bankmitarbeiter weist einen auf diese Problematik hin. Insoweit bedarf es einer größeren Transparenz und Überprüfbarkeit dessen, was hier entschieden wird. Denn auch wenn der Kunde die Wahl hat, welche Bank er besucht und die Bank die Wahl hat zu entscheiden, zu welchen Konditionen sie ein Kreditgeschäft macht (Erlebach S. 80), sollten die maßgeblichen Kriterien bekannt sein.

Der nunmehrige Gesetzentwurf der Bundesregierung zu mehr Tranzparenz beim Scoring (siehe Bundesratsdrucksache 548/08 zu einem Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes) verfolgt das Ziel, die Nachvollziehbarkeit der Verfahren zu verbessern und gleichzeitig mehr Rechtssicherheit und damit bessere Planungsmöglichkeiten für die Unternehmen zu schaffen. Er lag zum Zeitpunkt der Veranstaltung noch nicht vor, sondern nur der damalige Referentenentwurf. Der Referentenentwurf und das Scoring wurden zur Grundlage der vorliegenden Veranstaltung gemacht, auch wenn man von Titel her noch mehr hätte erwarten dürfen. Referenten waren der Philosoph Prof. Dr. Höffe, welcher sich zunächst zur Privatheit äußerte, Herr Huseman (Chief of Staff der Federal Trade Commission in den USA), welcher über den Identitätsdiebstahl berichtete, Herr Dr. Wuermeling, der über Europa als Rechtsrahmen für die deutsche Wirtschaft berichtete, Herr Brevoort (Senior Economist der Fed USA) der über das Kredit-Scoring und die Verfügbarkeit und Erschwinglichkeit von Kredit einen Vortrag hielt, der ehemalige Berliner Datenschutzbeauftragte Herr Prof. Dr. Garska, der sich zur datenschutzrechtlichen Seite äußerte, Herr Erlebach von der Commerzbank, der zur Risikosteuerung – Balance zwischen Kreditwirtschaftspraxis und Datenschutzgesetz, Unternehmens- und Kundeninteresse oder – wie transparent kann eine Kreditvergabe, wie transparent muss der Kunde sein? referierte, Herr Ulbricht von dem Verband der Vereine Creditreform, welcher über die Folgen der BDSG-Novelle für die Wirtschaft im Allgemeinen und die Auskunfteien im Besonderen referierte, sowie Herr Prof. Dr. Taeger zu dem Thema, was wird wirklich in diesem Entwurf für die Novelle des BDSG angestrebt. Daneben gab es für die Diskussion außer der Diskussionsleiterin noch zwei Kommentatoren, Herrn Pauli vom Bundesverband der Verbraucherzentrale und Herr Prof. Dr. Schierenbeck.

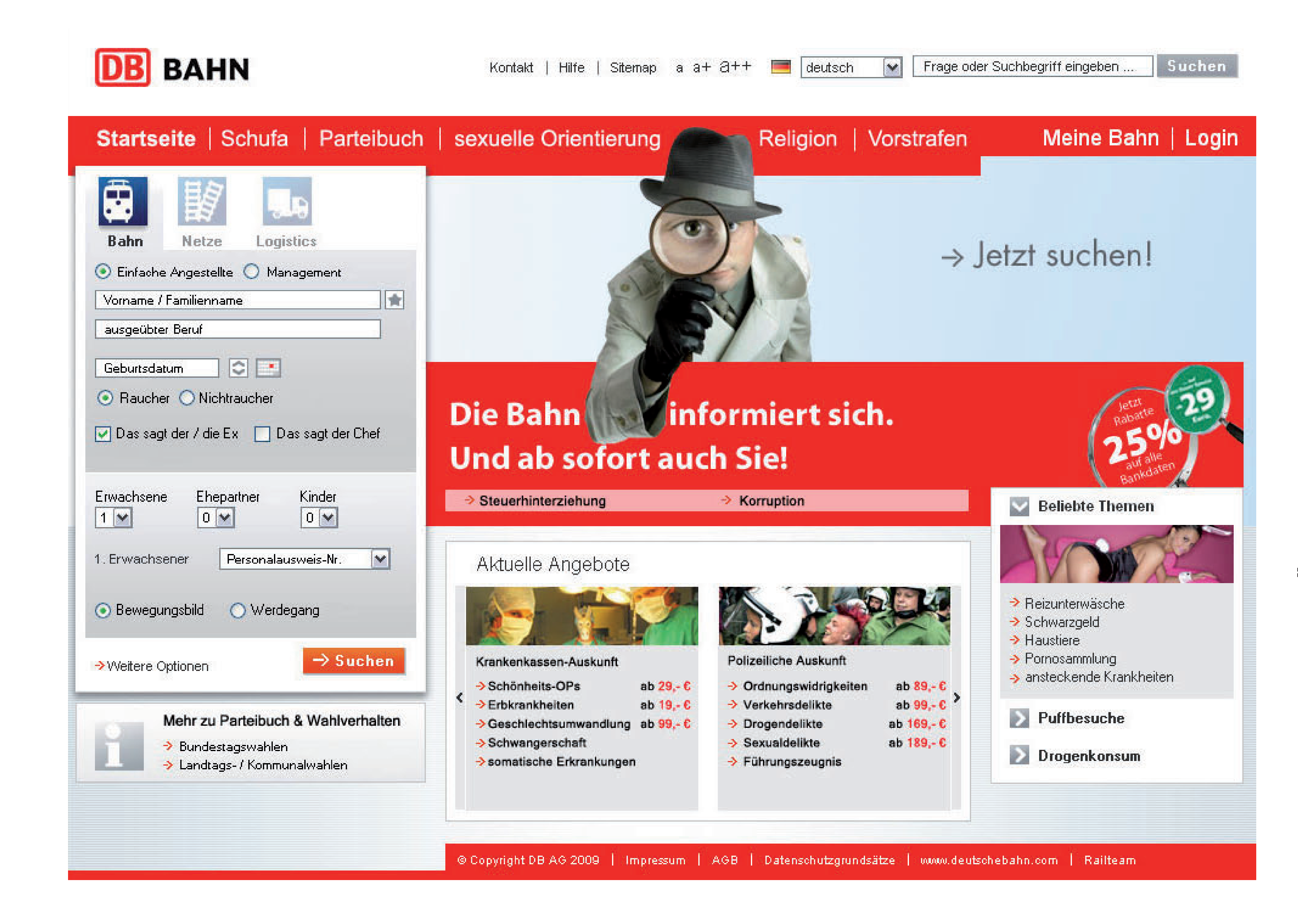
Die ganztägige Veranstaltung ist auf der DVD-Ausgabe auf zwei DVD's ansehbar und hörbar, wobei die Beiträge, soweit sie in Englisch gehalten wurden nicht simultan übersetzt werden. Es handelt sich um eine unkommentierte Aufzeichnung des Tagungsverlaufes. Demgegenüber ist die Buchfassung in Deutsch gehalten – ohne englische Beiträge, aber mit Anglizismen.

Ein roter Faden aus den Impulsreferaten und Initialreferaten ist – wie auch bei den Diskussionsbeiträgen, an denen die Zuhörer teilhaben durften – nicht durchgehend erkennbar. Auffällig ist jedoch, dass in dem gedruckten Band einzelne Textstellen farblich hervorgehoben wurden. Je nach Betrachtung handelt es sich um die Stellen, die für die SCHUFA als Argumente gegen den Gesetzgeber wohl eher positiv schienen. Dabei fällt auch auf, dass viele der Diskutanten manches gar nicht verstehen wollten, ist doch ihr Blick festgelegt. Insoweit sind sehr wohltuend insbesondere die Beiträge von Garska zu hören und zu lesen. Auch wies Herr Pauli vom Bundesverband der Verbraucherzentralen auf viele interessante Aspekte hin, wie den, dass wir, wenn wir mit Automaten arbeiten müssen, anfangen die Kontrolle zu verlieren über das, was im Ergebnis damit passiert (S. 91). Oder anders formuliert: Automatisierung löst keine Probleme, Automatisierung automatisiert sie (Garska S. 89). Von weitreichender Bedeutung ist aber auch die Aussage, dass das Kompetenzniveau für die Richtigkeit einer Score-Aussage nie über 90 % hinausgehen wird (Schierenbeck S. 70). Insoweit fragt man sich, wieso bei einer so hohen Fehlerquote (mindestens 10 %) der starke Glaube an die Score-Werte überhaupt möglich ist, soll doch das Wohl und Wehe der Bankenwelt und der Wirtschaft davon abhängen. Diese Frage wurde leider nicht weiter vertieft.

Alles in Allem ist mit dem vorliegenden Buch bzw. den beiden DVD's eine Veranstaltung dokumentiert worden, die sich in dieser oder ähnlicher Form und Zusammensetzung schon oft wiederholt hat und immer weiter wiederholen wird, ohne von Seiten der Betroffenen Score-Anwender und -Anbieter auf das eigentliche Problem einzugehen, dass nämlich nach Art. 15 EG-Datenschutzrichtlinie jeder Person das Recht einzuräumen ist, keinen für sie erheblichen beeinträchtigenden Entscheidungen unterworfen zu werden, die ausschließlich auf Grund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, und wenn doch, Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festgelegt werden. Und das ist nichts anderes als Transparenz und Auskunft über die Daten, die der Entscheidung zugrunde gelegt wurden.

Die DANA-Redaktion dankt der Redaktion des Titanic-Magazins für die Erlaubnis zum Abdruck der Bahnauskunfts-Grafik.

http://www.titanic-magazin.de



Quelle: http://www.titanic-magazin.de/uploades/pics/0204-bahnauskunft.jpg